Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

ӘОЖ 004.056.5 Қолжазба құқығында

ЖЕКАМБАЕВА МАЙГҮЛ НЕСІПАЛДЫҚЫЗЫ

Ақпараттық ресурстардың қауіпсіздік қатерін бағалау мен анализдеу әдістері

6D070400 – Есептеу техникасы және бағдарламалық қамтамасыз ету

Философия докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

техника ғылымдарының докторы,
профессор Б.С. Ахметов
техника ғылымдарының докторы,
профессор А.Г. Корченко
Ғылыми кеңесшілер

Қазақстан Республикасы
Алматы, 2017

МАЗМҰНЫ

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

АЖ – автоматтандырылған жүйе;
АҚ – ақпаратты қорғау;
АБ – ақпараттық белсенді;
АР – ақпараттық ресурстар;
АЖ – ақпараттық жүйе;
АТ – ақпараттық технологиялар;
С – сандық;
ҚСҚКМ-қауіп сипаттама қорының кортежді моделі ;
Сап– сапалы;
КСЖ – кешенді сарапшылық жүйе;
ЛА – лингвистикалық айнымалы;
АЕАО –анық емес арифметикалық операциялар;
ҚЖБ – қол жетімділіктің бұзылуы;
ҚБ – құпиялылықтың бұзылуы;
АЕЖ– анық емес жиынтық;
РҚЖ – рұқсатсыз қол жеткізу;
РЕМ – рұқсат етілмеген модификациялау;
ТБ – тұтастықтың бұзылуы;
АЕС – анық емес сандар;
ҚатБ – қатерді бағалау;
ҚҚБ – қауіп-қатерді бағалау;
ДК – дербес компьютер;
ПҚ – программалық қамтамасыздандыру;
ПҚ – программалық құралдар;
ТЖ – тұтынушылар жобасы;
АЖР – ақпараттық жүйе ресурсы;
ҚТП – қатер туғызушы потенциал;
ҚБАҚ – қатерді бағалау мен анализдеу құралдары;
АҚЖ –ақпаратты қорғау жүйесі;
АҚМЖ –ақпараттық қауіпсіздік менеджментінің жүйесі;
ТС –тақырыптық сауалнама;
СҚД – сипаттама қорының деңгейі;
ҚД– қатер деңгейі;
ҚФ – қатыстық функциясы;
МО – мақсатты объекттер.

КІРІСПЕ

Жұмыстың өзектілігі. Кәсіпорынның IT-инфрақұрылымының қарқынды дамуы ақпараттық ресурстардың (АР) әлсіздігі мен қауіп-қатер санының өсуін бақылай алмайтындыққа алып келеді. Мұндай жағдайда ақпараттық қауіпсіздік қатерін бағалау ақпаратты қорғаудың (АҚор) қажетті деңгейін анықтауға, оны қолдауды жүзеге асыруға және объектті қорғаудың ақпараттық құрылымын дамуының стратегиясын өңдеуді жүзеге асыруға мүмкіндік береді. Қатерлерді басқару жүйесін және ақпараттық қауіпсіздік қамтамасыз ету бойынша жұмыстардың жоспарын жасаған кезде қатерді бағалау мен анализдеу қажетті шарттылық болып табылады [1-8].

Кез келген меншік түріндегі кәсіпорында ақпараттық қауіпсіздікті қамтамасыз ету үшін ISO/IEC 27001 стандартының ұсынысы бойынша ақпараттық қауіпсіздік менеджментінің жүйесін (АҚМЖ) енгізу қажет [9]. Қатер менеджменті мұндай стандарттың негізі болып табылады, мұның астында ақпараттық қауіпсіздік қатерін өңдеу, бағалау мен анализдеу тұспалданады. Қазіргі кезде, бағалау үшін қолданылатын, айтарлықтай кең спектрде берілген яғни нормативті құжаттардан (стандарттардан) басталып, нақты программалық қосымшалармен аяқталатын қатерді бағалау мен анализдеудің көптеген құралдары (ҚБАҚ) бар [1, 3, 4, 7, 10-12]. Практикалық қызметте қолдану үшін соңғыларын таңдау кезінде сарапшы көптеген сұрақтармен соқтығысады, мәселен, мынадай, «Қандай параметрлерді қолданған жөн?», «Қанадай математикалық аппарат қолданылады?», «Статистикалық мәліметтерсіз қалай бағалауға болады?», «Анық емес шарттылығында қатерді бағалау мен анализдеуді қалай жүзеге асыруға болады?» т.б. Осы және өзге факторлар сәйкес келетін бағалау амалын таңдау кезінде бірқатар қиындықтар туғызады. Сонымен бірге, айта кететін жайттардың бірі, негізінде ақпараттық қауіпсіздік қауіп-қатерлері мен оқиғалары туралы статистикалық мәліметтер қатерді бағалау мен анализдеу үшін қолданылады. Көптеген елдерде (соның ішінде Қазақстан да) осындай статистиканы [7] тіркеу мен қолдануға қатысты мемлекеттік айла-құралдар жоқ, бұл өз кезегінде мемлекетте қолдану үшін бар болған құралдардың мүмкіндігін шектейді. Сарапшының қатерді бағалау кезінде параметрдің кеңдеу спектрін қолдану мүмкіндігін қиындататын және бір фактор – бұл осындай құралдарда белгілі бір шектеулердің (қолданылып жатқан параметрлер жиынына) бар екендігі болып табылады, бұл өз кезегінде олардың икемділігін төмендетеді.

Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу әдістерін дамытуда айтарлықтай үлес қосқан отандық ғалымдар: Л.Б. Атымтаева, Б.С. Ахметов, Б.Б. Ахметов, У.А. Тукеев және басқалар [2, 13-18]. Шетел ғалымдары арасында осы салада белсенді жұмыс істеушілер мыналар: А. Г. Корченко, Д. Д. Костров,С. А. Петренко, Т. Р. Пелтиер, В. К. Маршалл, И. С. Медведовский, Э. Мушик, С. А. Нестеров, С. В. Симонов, Ф. Рагозин, П. Фишберн [7, 10, 12, 19-27], т.б.

Бірақ ақпараттық қауіпсіздік қатерін басқару саласында шешімі тәжірибелік және ғылыми маңызды мәнге ие біраз тапсырмалар мен проблемалар қалып отыр. Міне осы позиция жағынан, ҚБАҚ және әдістерді зерттеу мен өңдеу ақпараттық қауіпсіздік қатерін бағалау мен анализдеу аспаптарын қолдану кезінде айтарлықтай икемді (құрылғылар) (саланы, кәсіпорынның экономикалық және басқарушылық ерекшеліктерін, уақытты т.б. есепке ала отырып) жасауға мүмкіндік беріп, статистикалық мәліметтер, сонымен қатар, анық емес, әлсіз қалыптасқан ортада жасалған сарапшылық бағалаулар негізінде сәйкес келетін тапсырмаларды тиімді шешуі көкейкесті ғылыми мәселе болып табылады.

Зерттеудің мақсаты мен міндеттері. Диссертациялық жұмыстың мақсаты мен әдістері сипаттама қорының кортежді моделін (ҚКМ) қолдану негізінде бағалаудың икемді құралдарын жүзеге асыруға мүмкіндік беретін ақпараттық қауіпсіздік ҚБАҚ мен әдістерді өңдеу болып табылады.

Қойылған мақсатқа қол жеткізу үшін келесі негізгі міндеттерді шешу қажет:

1. Ақпараттық қорғаудың тапсырмаларын шешуде тиімдірек аспапты жасау мен таңдау үшін қолданылатын сипаттама қорының жинағын анықтау мақсатында қатермен байланысты негізгі түсініктерді, бар болған стандарттарды, әдістерді, әдістемелерді, әдіснамаларды және программалық ҚБАҚ-ды зерттеу мен талдау;
2. Алынған сипаттама қоры негізінде көлемнің жиынтығын динамикалық анықтауға мүмкіндік беретін қордың кортежді моделін (ҚКМ) өңдеу және осылай сәйкесінше ақпараттық қауіпсіздік ҚБАҚ өңдеуде икемділікті қамтамасыздандыру;
3. Қордың кортежді моделі (ҚКМ) есебінен бағалаудың тиімді құралдарын жасауға мүмкіндік беретін, анық емес анықталған сипаттама қоры мен детерменттелген жиынтығын динамикалық түрде өзгертетін кіріс мәліметтер түрінде қолданылушы ақпараттық қауіпсіздік қатерін бағалау мен анализдеу әдісін өңдеу;
4. Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу тапсырмаларын шешу кезінде *n*-еселі инкременттелген эталонды параметриялық трапеция түріндегі және үшбұрышты анық емес сандарға (АЕС) негізделетін лингвистикалық айнымалы (ЛА) тәртібін (термдер санын) эквивалентті түрде алдын ала анықтауға мүмкіндік беретін әдістерді өңдеу. Бұл көрсетілген жүйелердің әрі қарай дамуына септігін тигізеді және олардың трапециялық түрегі және үшбұрышты анық емес сандарын қолдану құралдары бойынша мүмкіндіктерін кеңейтеді;
5. Ұсынылған әдістер мен модельдер қолданылған, қатерді тиімді бағалауға арналған программалық сияқты программалық-аппаратты жүйесінің құрылым процесін нысандандыру мен жинақтап қорытуға мүмкіндік беретін, Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу жүйесін синтездеу әдіснамасын өңдеу;

6. Ақпараттық қатерлер саласындағы мәселелерді шешу үшін ұсынылған әдістерді, модельдері және әдіснамаларды қолданатын жүйелердің жаңа құрылымдық шешімін өңдеу;

7. Бар болған жүйелердің ұсынылған әдіснамасы мен құрылымдық сұлбасы негізінде өңделген әдістерді, моделі мен құрылымдық шешімдерін тексеру мақсатында программалық ҚБАҚ қамтамасыздандыруын программалық қамтамасыздандыру (ПҚ) эксперименталді зерттеуді жүзеге асыру мен өңдеу;

Зерттеу объектісі – Ақпаратық қауіпсіздік қатерді бағалау мен анализдеу процесі.

Зерттеудің пәндік аймағы – Ақпараттық қауіпсіздік саласындағы қатарді бағалау мен анализдеу құралдарының программалық құралдары, әдістері, жүйелері, модельдері және әдістемелері.

Зерттеу әдістері. Жүргізілген зерттеулер анық емес логика теориясының заманауи әдістеріне (қатерді бағалау мен анализдеу әдістерін өңдеу, сонымен бірге лингвистикалық айнымалының терм санын *n*-еселі инкременттеу әдісін өңдеу), алгоритмдер шешімін қабылдауға, бағытталған-объектті программалау (ақпараттық қауіпсіздік ҚБАҚ ПҚ өңдеу), ақпараттық процесстер мен құрылымын еліктеп моделдеуге (эксперименталді зерттеуді жүргізу кезінде ақпараттық жүйе жай-күйінің ортасы мен әр түрлі шарттылықтарын модельдеу), сонымен бірге жайлы есептеуге негізделеді.

Зерттеудің ғылыми жаңалықтары келесіде өз шешімін табады:

- алты компоненттік кортежбен бейнеленген сипаттама қорын талдап қорыту есебінен талап етілетін сипаттамалар жинағының жиынтығын қалыптастыру мүмкіндігін есепке алатын қатерді бағалау мен анализдеудің тиімді, әрі икемдірек әдістерін жасауға мүмкіндік беретін алғаш рет қатердің сипаттама қорының кортежді моделі өңделді;
- мұнан былайғы дамуды алдық қатерді бағалау мен анализдеу әдістері детерменттелген және анық емес анықталған параметрлер қоры жинағының динамикалық түрде өзгеруін өңдеудегі логикалық-лингвистикалық айнымалы және қатердің сипаттама қорының кортежді моделі есебінен бағалаудың интеграцияланған мүмкіндігі бар тиімді амалын жасауға мүмкіндік береді;
- бірінші және екінші жеке қор кеңейуін қолданумен n-еселі инкременттелген терм сандарының функциясын жүзеге асыру әдісін алғаш рет өңдеу; мұнда термдерді бір тәртіпке инкременттеу функциясын *n*-еселі кеңейту модификациясының есебінен сарапшыларды сәйкесінше құрал-жарақ саласына жұмылдырусыз n тәртіптерге лингвистикалық айнымалы термдерінің эталонды санын эквивалентті трансформаторлау процесін қалыптастыру мүмкіндігі кеңейеді;
- Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу кезінде өңделіп жатқан көлемінің берілген жиынтығын қолданудың икемденгіш мүмкіндігі бар аспаптық құралдарды жасау процесін қалыптастыруға мүмкіндік туғызатын ақпараттық қауіпсіздік қатерін бағалау мен анализдеу жүйесін синтездеу мұнан былайғы дамуды алдым әдіснамасы;

- мұнан былайғы дамуды алдық ақпараттық қауіпсіздік қатерін бағалау мен анализдеу жүйесінің құрылымдық шешімі ұсынылған әдістерін жүзеге асырушы мәліметтерді қалыптастыру мен сипаттама қорының өңделген ішкі жүйесі есебінен мәліметтерді сапалық, әрі сандық интерпретациялау түрінде қайта жаңғырту мен қалыптастыруға мүмкіндік береді;

Жұмыстың практикалық құндылығы мыналарда өз көрінісін тапқан:

- ұсынылған синтездің өңдеу әдіснамасының және жүйелердің құрылымдық шешімі негізінде ақпараттық қауіпсіздік программалық ҚБАҚ-н жүзеге асуы үшін алгоритм түзілген;

- ҚБАҚ құру кезінде қолданыуға болатын бұзылған ақпараттық қауіпсіздіктің қауіп-қатері мен оқиғасының , АР-дың біріктірілген мәліметтер қоры өңделген;

- ұсынылған алгоритм мен біріктірілген мәліметтер қоры негізінде сипаттама қорының әр түрлі жинағын динамикалық түрде анықтайтын және қолданатын, детерминдендірілгенде де, анық емес, әлсіз құрастырылған ортада да икемдігін, функционалдығын және оны қолдануда ыңғайлылығын көтеретін, ақпараттық қауіпсіздік ҚБАҚ-дің қолданбалы программасы жүзеге асырылады

Зерттеу нәтижелері Қ.И.Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университетінің «Ақпараттық қауіпсіздік» кафедрасы, Ұлттық авиациялық университетінде (Киев қаласы, Украина) «Ақпараттық технологиялар қауіпсіздігі» кафедраларында оқу процессінде қолданылды сонымен қатар «Ақпараттық технологиялар қауіпсіздігі» «ДЕЛЬТА» (Киев қаласы, Украина) және ЖШС «QUARES» (Алматы).

Диссертацияның апробациялық шешімдері. Диссертациялық жұмыстың негізгі тәртіптері мен нәтижелері ғылыми-техникалық конференциясында, семинарларда, баяндалды және талқыланды сонымен бірге;

– Қ.И.Сәтбаев атындағы ҚазҰТЗУ-дың «Ақпараттық қауіпсіздік» кафедрасында «Ақпаратты қорғаудың қазіргі заманғы технологиялары» ғылыми семинарда;

– Ұлттық авиациялық университетінің (Киев қаласы, Украина) «Ақпараттық технологиялар қауіпсіздік» кафедрасының ғылыми семинарында;

– Қ. И. Сәтбаев атындағы ҚазҰТУ-ң 80 жылдығына арналған «Қазақстан-2050» Стратегиясынын іске асырудағы жас ғалымдардың орны мен рөлі» атты Халықаралық Сәтбаев оқулары Алматы, 2014ж.;

– «Ақпараттық және телекоммуникациялық технологиялар. Білім, ғылым, тәжірибе атты II Халықаралық ғылыми-тәжірибелік конференциясы Алматы, 2015ж.;

– Қ. И. Сәтбаев атындағы ҚазҰТУ-ң 80 жылдығына орай «XXI ғасырдағы инженерлік білім және ғылым: проблемалары мен келешегі» атты халықаралық форумы, Алматы, 2014ж.;

– Л.Н.Гумилев атындағы Еуразия ұлттық университеті «Казахстан-2050» Стратегия аясында «Ақпараттық қауіпсіздік» III Халықаралық ғылыми-практикалық конференция, Астана, 2015ж.;

– XV Халықаралық ғылыми-тәжірибелік конференция «Білім берудегі информатика мәселелері, басқару, экономика және технологиялар», Пенза, 2015ж.;

– Second International Scientific-Practical Conferenc «Problems of Infocommunications. Scienceand Technology», Kharkiv, 2015;

– II международная научно-практическая конференция «Актуальні питання забезпечення кібернетичної безпеки та захист інформації», Киев, Европейский университет, 2016.

– Халықаралық ғылыми-тәжірбиелік конференция «Макроэкономикалық талдау және экономикалық саясат жөніндегі математикалық тәсілдер және ақпараттық технологиялар» (академик А. Әшімов 80 жылдығына орай), Алматы, 2017ж.

Диссертациялық жұмыс Қ.И. Сәтбаев атындағы ҚазҰТЗУ ғылыми-зерттеу жобасының аясында жүзеге асырылды №757.МОН.ГФ.15.ИИТ.6 «Ақпараттық қауіпсіздік Биометрикалық стандарттар қолдау жөніндегі ғылыми-зерттеу, үйлестіру, өзгерту және тіркеу» және Ұлттық авиация университетінің Украина, Киев қаласы «Ақпараттық жүйелердің қауіпсіздік қатерін бағалау әдістемесі» ғылыми-зерттеу жұмысы (тіркеу №14.01.05 нөмірі 105).

Мақалалар. Диссертациялық жұмыстың тақырыбы бойынша 16 ғылыми жұмыс жарияланды оның ішінде; 5 мақала ҚР БжҒМ Білім саласындағы бақылау комитеті ұсынған журналдарда жарияланғанды, 1 мақала Дерекқор Scopus деректер базасына (Elsevier) индекстелген журналында жарияланды; 10 мақала Халықаралық конференциялар материалдарында жарияланды; оның ішінде 5-шет елдегі конференция, 1-тезис жарияланды.

Диссертацияның құрылымы мен көлемі. Диссертациялық жұмыс, кіріспеден, төрт бөлімнен, қорытындыдан, 85 пайдаланылған әдебиеттер тізімінен тұрады; барлығы 150 бетте көрсетілген, 43 суреттен, 58 кестеден және қосымшадан тұрады.

1 АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРІН БАҒАЛАУ МЕН АНАЛИЗДЕУ ҚҰРАЛДАРЫ

1.1 Қатерді анықтау анализі

Әдебиеттерде қатерді анықтау **әрекет немесе қызмет** түрінде кездеседі: оның жүзеге асырылуы қандай да бір айтарлықтай маңызды қажеттілікті қанағаттандыруды қауіп-қатерге қояды [28]; оның нәтижесінің анық еместігінен және субъект үшін сәтсіз жағдайда мүмкін болған жағымсыз салдардан тұратындығы [29, 30]; анау немесе мынау жағдайда субъектке шығын (ұтылу, жарақаттану, зақымдану) қауіпін төндіреді [30, 31]; субъект қызметі белгісіздік жағдайында белгісіздікті [32]; сәтті нәтижеге жету мақсатына байланысты созумен байланысты [28].

Әрекет немесе **қызмет** [33] **ықтималдылық** (өлшенетін немесе есептелетін) сияқты олардың өздеріне ғана тән оқиғаның пайда болуымен байланысты екені барлығына белгілі. Сонымен бірге, «оңды» мүмкіндіктер сияқты «қауіпті» ықтималдылықтарды да беруі мүмкін кез келген әрекет оқиғалар мен салдарға алып келетіні белгілі [32]. Айтылғандардың нәтижесінде, бұл контекстте көрсетілген түсініктердің жалпылығы бақыланады.

Келесі сипаттамалық қорды "**оқиға"**болуы мүмкін немесе болмауы мүмкін [32, 34] немесе оның болуын күту (белсендіге потенциалды жағымсыз әсерлер немесе оның бұрынғының, болашақтың немесе қазіргі кездің салдары болып табылатын сипаттамалары [35, 36]) түрінде қарастыруға болады.

Көрсетілген көптеген дерекнамаларда қатер ықтималдылық немесе онымен байланысты түсініктермен бейнеленеді, мысалы, **өлшенетін немесе есептелетін ықтималдылықтар:** қауіпсіздігінің потенциалды бұзылу мүмкіндігін тұспалдайтын [32, 36-38]; берілген қауіп-қатердің пайда болуы және осы қауіп-қатердің пайда болу салдарының потенциалды сәтсіздігі [36, 37]; осы қауіп-қатер дүние-мүлікті зақымдау және\немесе шығынға алып келу үшін белсендінің немесе белсенділер тобының әлсіз жақтарын [38, 39]; сонымен бірге, оқиға ықтималдығын және оның салдарын үйлестіру мен қисындастыру түрінде қолдану [28] қоршаған ортаға, дүние-мүлікке немесе өмірге (денсаулыққа), азаматтарға, жануарларға, өсімдіктерге зиянын тигізу [32, 36]; анықталған қауіп-қатерді, қауіп-қатердің түрін және зиянданған қауіп-қатер көлемін жүзеге асыру [32]; пайданы қолдан жіберіп алу немесе шығындалу (сәйкес келетін шығын мен пайданы алуда санды түрде өлшенетін сенімсіздік) [40]; қойылған мақсаттан күтілетін нәтижелерді алуға мүмкіндіктің болмауды немесе сенімсіздікті шарттайтын жағдайлардың пайда болуы [40, 41]; мақсатқа жетпеу [3, 36, 42, 43], қабылданып жатқан шешімнен нәтиже алу [41], оқиғаның (мысалы, мұның нәтижесінде күтілмеген жоғалудың пайда болу мүмкіндігінің ([44]) немесе қауіптің, сәтсіздіктің болу мүмкіндігінің [19], жағымсыз нәтиженің пайда болуын [45]; шығын [6, 7, 9, 46-49]; Ықтималдылық белгілі бір оқиғаның басталуымен байланыстылығы барлығына белгілі [50-52], сондықтан онымен мына жерде қатер де байланысты болып тұр.

Ытималдылықты жиі «объектіге» (кейде физикалық деп те атайды) және «субъектіге» [11] бөледі. Объективті ықтималдылық дегенде сәтті нәтижелер санының олардың жалпы санына қатынасы немесе жалпы бақылау көлемінде қандайда бір оқиға пайда болуының салыстырмалы жиілігі түсініледі. Мысалы, ол, бақылаудың үлкен санының шешімдерінің анализі кезінде қалыптасады. Субъективті ықтималдылық дегенде берілген оқиғаның болатындығы туралы кейбір адамдардың немесе адамдар тобы сенімділігінің өлшемі. Бұл ықтималдылық немқұрайлы әр түрлі тәсілдермен берілген болуы мүмкін, мысалы, ықтималды таралу немесе оқиғалар жиынтығында бинарлық қатынас тәсілімен берілген болуы мүмкін, бірақ сарапшылық жолмен алынған ықтималдылық өлшем түрінде өзін көрсетеді [11].

Сонымен бірге, қатерді **қауіп** түрінде бейнелейтін анықтаулар да кездеседі: болжанатын (белгілі) қазіргі сәтте белгісіз, бірақ пайда болуы мүмкін [42, 53]; шабуыл тәсілімен зияндандыру (белсенді немесе белсенділер тобының әлсіздігін қолданып, кейбір қауіп-қатерді жүзеге асыру [5]).

Қатерді анау немесе мынау оқиғаның пайда болуымен тікелей байланысты шығындалу немесе жұмсау жиілігі деп анықтайтын түсініктердің бар екені белгілі. Олардың бірнешеуін мысалға келтірейік, мысалы, қатер: шешімі, өзгелерімен салыстырғанда өзгеше, ұтымды болатындай шарттылығында белгілі бір шешімді жүзеге асырумен байланысты оқиға көлемін экономикалық әсерден оның мүмкін болған жұмсауы немесе шығындалуының өлшеміне көбейту нәтижесі түрінде [54]; «**қауіпті**» жүзеге келтіретін жиілік [55];. Сонымен бірге қатер кез келген контекстте қауіп-қатердің (яғни зиян келтіретін оқиға), әлсіздіктің (қауіп-қатерге кәсіпорындардың ашықтығы) және мал-мүлік құндылығының (қауіп кезіндегі белсендінің құндылығы) жиынтық көлемі түрінде қаралады. Осы факторлардың кез келгені ұлғайса, қатер де сәйкесінше ұлғаяды, ал төмендеуі оның кішірейуіне алып келеді [50, 56].

Адам өмірінің әр түрлі саласындағы қатер түсінігінің анализін жүргізгеннен кейін қатердің бір сипаттамасын ерекше көрсетуге болады, жоғарыда келтірілген барлық анықтамаларда кездесетін және оларды біріктіретін-оқиға, оқиға-бұл болуы керек болған және авторлардың ықтималдылықпен, әрекетпен немесе қызметпен, жиілікпен, шығынмен, қауіппен т.б. байланыстыруы.

Ақпараттық қауіпсіздік аспектінде қауіп-қатерді жүзеге асыру оқиғасына байланысты қатерді ақпараттық жүйе ресурстарына байланыстыруға болады, оның салдарынан олардың сипаттама қоры қауіпсіздігінің-құпиялылығының, тұтастығының, қол жетімділігінің бір немесе бірнеше бұзылулары болып өтті. Сонымен бірге, оны былай көрсетуге болады: сипаттама қауіпсіздігінің бұзылуына алып келген оқиға ықтималдығы; субъекттің бейәрекеттігі немесе қызметі-субъекттің қатысуымен немесе қатысуынсыз болған оқиға; белгілі бір жиілікте болып жатқан оқиға т.б.

Қатер түсінігін анықтап жатқан кезде АҚ бойынша көптеген шешімдер анық емес шарттылықта қабылданатынын есепке алу керек [57].

Жүргізілген анализ бойынша қатерді әр түрлі трактаттау жалпы сипаттама жиынтығына ие, мысалы, қатердің белгілі бір оқиғаның басталуымен және

ықтималдығымен байланысты т.б. Бұл түсінікті түсіндіру үшін АҚ саласында осы салаға қатысты оның сипаттама қорының жиынағын бөліп көрсету қажет.

Қойылған мәселені шешу үшін ақпараттық қауіпсіздік қатерлерін бағалау мен анализдеудің 27 түрлі қазіргі заманғы құралдары зерттерлген және анализ жасалған болатын олар келесі бөлімдерде көрсетіледі [58, 59].

Диссертациялық жұмыс Қ.И. Сәтбаев атындағы ҚазҰТЗУ ғылыми-зерттеу жобасының аясында жүзеге асырылды №757.МОН.ГФ.15.ИИТ.6 «Ақпараттық қауіпсіздік Биометрикалық стандарттар қолдау жөніндегі ғылыми-зерттеу, үйлестіру, өзгерту және тіркеу» және Ұлттық авиация университетінің Украина, Киев қаласы «Ақпараттық жүйелердің қауіпсіздік қатерін бағалау әдістемесі» ғылыми-зерттеу жұмысы (тіркеу №14.01.05 нөмірі 105).

1.2 Ақпараттық қауіпсіздік қатерін бағалаудың программалық құралдары

ҚБАҚ 1 - COBRA әдістемесі (Consultative Objective and Bi-Functional Risk Analysis, Ұлыбритания өңдеуші – C&A Systems Security Ltd**.** компаниясы) ақпараттық белсенділер және компанияның электрондық бизнес транзакция қатерлерін бағалау барысында қолданылатын тақырыптық сауалнама (check list’s) арқылы ISO 17799 стандарт талабын қолдауға бағдарланған [60, 61]. Сарапшылық жүйені құру принциптері негізінде өңделген қауіпсіздік амалын жүргізу мен консалтинг үшін өнім аспаппен кеңейтілген. Программалық қамтамасыздандыру (ПҚ) комплектіне қаруландыратын білім қорын өзгерту мен жөндеу үшін қолданылатын COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst және COBRA Data Protection Consultant модульдері кіреді.

Тақырыптық сауалнама инициализациясы негізінде қатерді бағалау мен анализдеу төмендегі категориялар бойынша жүзеге асырылады: жоғары деңгейлі; ақпараттық технологиялар қауіпсіздігі (АТ); оперативті ақпараттық технология және бизнес; электронды коммерция инфрақұрылымы. Тақырыптық сауалнама модульдері бөлек үстемелерді ақпаратты түрде қолдайды, мысалы: APP-MAN (Application level security management) – қауіпсіздікті басқару; APPAUDIT (Application level Auditing) – аудит; APPCNTRL (Application Staff control) – штат бақылау; APPDEPND (Application Staff dependency) – штат тәуелділігі; AUDIT (System Audit) – жүйенің тексеруі т.б. APPCNTRL үшін мәліметтерді инициализациялаудың мысалы ретінде – «Соңғы 2 жыл ішінде ұрлықтың неше қақтығысы болды?» сұрағы арқылы осындай қақтығыстардың оннан аса саны кезінде «10» саны енгізілуі мүмкін.

Сұрақтан көрініп тұрғандай мұнда ұрланған туралы дәлелдеу жоқ, бұл қамданудың дәрежесін және анау немесе мынау қақтығыс қандай ақпараттық жүйе (АЖ) ресурстарының қауіпсіздік сипаттамасына әсер еткендігін анық анықтауға мүмкіндік бермейді. Мұндай тәсіл қатерді айтарлықтай тұрпайы бағалауды ғана жүзеге асыруға мүмкіндік береді. Ұрлық ([19] есепке ала отырып) бұл типтегі субъекттелген белсенді қауіп-қатер, мұндай жағдайда мысалы, белгілі бір ақпараттық ресурстардың жалғыз экземплярының

жоғалуымен, ұрлық сонымен бірге, мәліметтердің енбестен алдын немесе енгізу кезінде ауыстырылып қоюымен т.б.құпиялылық, тұтастық және қол жетімділік бұзылады (ҚТҚЖ) [19]. Құпиялы ақпараттың ұрлану кезінде компанияның тартатын шығындарының деңгейіне қатысты, мысалы, қызметкерлердің жеке ақпараты немесе клиенттердің мәліметтер қоры мұндай оқиғалар басталған кезінде айтарлықтай ерекшеленіп тұрады.

Инициализацияланған мәліметтерді өңдегеннен соң жүйе есепті түрлендіреді, (Detailed Risk Assessment (continued)) бағасы детальді түрде келесі қатер сипаттамасы бойынша суреттеледі: (RISK CATEGORY) категориясы; (RISK LEVEL) деңгейі; (RISK ASSESSMENT) бағасы. Мысалы: ҚАТЕР КАТЕГОРИЯСЫ – «Бизнестегі күтілмеген жағдай»; ҚАТЕР ДЕҢГЕЙІ – 96,61%; ҚАТЕР БАҒАСЫ – «Қызметкерлер құрамы күтілмеген жағдайға жаман дайындалған, күтілмеген жағдайлардағы әрекеттің жоспары жоқ және осыларға талаптар орындалмайды».

Қатерді бағалау мен анализдеу тақырыптық сауалнама арқылы инициализацияланған мәліметтерді өңдеу болады.

Барлық категорияларды суреттегеннен және қатер деңгейін (ең жоғарғыдан нольге дейін) саралағаннан кейін әдістемеде оларды төмендету бойынша ұсынылатын шаралар келтіріледі. Осылай келтірілген мысалда, қатердің берілген категориясы үшін ұсыныс беріледі – «Тұтынушылар ресми түрде өздерінің қызметтерінің минималды талабын анықтау керек және күтілмеген жағдайларға дайын болуы керек». Сонымен бірге, әдістемеде тақырыптық сауалнама (Question & Response Listing (continued)) үшін инициацияланған мәліметтерді қарау мүмкіндігі бар.

ҚБАҚ 2-техникалық түрдегі (мысалы, АТ құрылғылары мен программалық қамтамасыздандыру) сияқты және техникалық емес (мысалы, физикалық немесе адамдық) сипаттағы қауіпсіздік аспекттерін, қатерді бағалау мен анализдеуге қатал және кезеңдік тәсіл қарастырылған аттас программалық өнімінде Insight Consulting Limited фирмасында **CRAMM** (CCTA Risk Analysis and Management Method, өңдеуші –Телекоммуникация және компьютер бойынша орталық агенттігі (CCTA – Central Computer and Telecommunications Agency), Ұлыбритания**) әдісі** жүзеге асырылған [62, 63]. Келесі кезекте бағалау процесі үш кезеңде жүзеге асатын CRAMM құралының аспаптық программасын қарастырастырамыз. Біріншісінде – жүйенің ішкі жегінде тұратын, ақпараттық және программалық, физикалық ресурстардың идинтификациясы жүргізіледі. CRAMM-дағы физикалық ресурстар бұзылған жағдайда, олардың құндылығын, оларды қайта қалыптастыру құны анықтайды. мәліметтер мен ПҚ үшін берілген АЖ критериясында қолданылатындар таңдалады, 1-ден 10-ға дейін мәндер шкаласы бойынша зиян бағасы беріледі. Мысалы, «ресурсты қайта қалыптастырумен байланысты қаржылық шығын» критериясы бойынша шкала бағасы келесі мәндер арқылы бейнеленеді [1,12]: 2 балл – $1000-дан аз; 6 балл – $1000-дан $10 000-ға дейін; 10 балл-$100 000 жоғары т.б.

Екінші кезеңде ресурстар тобы мен олардың әлсіздіктері үшін қауіп-қатер деңгейін бағалау мен идентификация жайлы барлығы қарастырылады. Тұтынушы сервистердің белгілі бір ресурс топтарынан тәуелділігі және әлсіздіктер мен қауіп-қатердің бар болған деңгейі бағаланады, сонымен бірге, қатер деңгейі есептеледі де, нәтижелері анализденеді. Ресурстар әлсіздіктер мен қауіп-қатер типтері бойынша топтастырылады. Мысалы, ресурс тобына қатысты бар болған ұрлық немесе өрт қауіп-қатері жағдайында бір жерде (сервистік зал, байланыс құралдарының бөлмесі т.б.) орналасқан барлық ресурстарды қарастыру орынды болар еді.

CRAMM программалық құралы әрбір ресурс тобы үшін (әрбір 36 қауіп-қатер типінен) сұрақтар тізімін түрлендіреді де, олар үшін инициализациялаудан кейін деңгей бағасы мысалы, өте жоғары, жоғары,орташа, төмен, өте төмен (қауіп-қатер үшін) түрінде және жоғары, орташа, төмен (әлсіздіктер үшін) түрінде жүзеге асырылады. **«Қауіп-қатер бағасы»** үшін сұрақ үлгісін қарастырайық: «Соңғы үш жыл ішінде ұйым қызметкерлері басқа тұтынушылардың құқығын қолданып АҚор сақталынатын ақпаратты рұсқсат етілмеген қол жеткізумен алуға талпынды?» Сонымен бірге, әрі қарай өңдеу үшін сұранысқа мәліметтерді инициализациялау нұсқалары белгілі бір балдар санымен ұсынылады: a) ешқашан (0 балл) емес; … d) орташа жиілігі жылына бір рет (30 балл) т.б. **«әлсіздіктің бағасына»** сұраныс үлгісі: «АЖ-ні қанша адам қолдануға құқылы?» a) 1-ден 10-ға дейін (0 балл); b) от 11-ден 50-ге дейін (4 балл) т.б. Осы ақпараттың негізінде 1-ден 7-ге дейінгі градациялы дискреттік шкалада қатердің деңгейі (қатерге зиян келтіре алатын [1] қандайда бір әрекет немесе оқиға нәтижесінде шығын мүмкіндігі түрінде анықталады) есептеледі. CRAMM программалық құралы қатер матрицасында қауіп-қатер мен әлсіздіктерді шкалаларды жасау үшін біріктіреді, мысалы, (әлсіздіктер мен қауіп-қатер деңгейі үшін) 1.1 кестесі қолданылады.

Кесте 1.1 - Әлсіздіктер мен қауіп-қатер деңгейі үшін шкалалар

Шкалалар	Сипаттамасы	Мәні
1	2	3
Қауіп-қатер деңгейінің бағалау шкаласы (пайда болу жиілігі)	Инцидент (қақтығыс) орташа әр 10 жылдан жиі емес болады.	өте төмен
	Инцидент (қақтығыс) 3 жылда орташа бір рет болады.	төмен
	Инцидент жылына орташа бір рет болады	орташа
	Инцидент 4 айда орташа бір рет болады	жоғары
	Инцидент айына орташа бір рет болады	өте жоғары
Әлсіздіктер деңгейінің бағалау шкаласы (қауіп-қатердің сәтті жүзеге асуы ықтималдығы)	Инцидент пайда болған жағдайда ең төмен сценарий бойынша оқиғаның даму ықтималдығы 0,33-тен кем	төмен
	Ицидент пайда болған жағдайда ең төмен сценарий бойынша оқиғаның даму ықтималдығы 0,33-тен 0,66-ге дейін	орташа

	Ицидент пайда болған жағдайда ең төмен сценарий бойынша оқиғаның даму ықтималдығы 0,66-ден жоғары	жоғары
	Ицидент пайда болған жағдайда ең төмен сценарий бойынша оқиғаның даму ықтималдығы 0,33-кем	төмен

АЖ қорғайтын ресурстар құнының бағасынан шыға отырып, «күтілетін жылдық шығындалулар» анықталады. 1.1 суретінде күтілетін шығындалулар бағасының матрицасы келтірілген [1], мұндағы сол жағындағы екінші бағана ресурс бағасының мәнін құрайды, ал кестенің жоғарғы басты жолы – бір жыл мерзімінде қауіп-қатердің пайда болу жиілігінің (қауіп-қатер деңгейінің) бағасы, төменгі басты жол – қауіп-қатерді жүзеге асырудағы сәттілік ықтималдығының (әлсіздік деңгейінің) бағасы.

		0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
		0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

Сурет 1.1 - Күтілетін жылдық шығындалулар матрицасы.

Күтілетін жылдық шығындалулар мәні (Annual Loss of Expectancy) қатер деңгейін көрсететін балға өтеді, осыған сәйкес 1.2. суретінде берілген (бұл мысалда шығындалулар көлемі фунт стерлингте берілген) шкалалар әрі қарай матрицаға (1.3 суретте) сәйкес қатердің бағасы шығарылады.

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

Сурет. 1.2 - Баға шкаласы

Зерттеудің үшінші кезеңі адекваттық контршараларды іздеумен қорытылады. Мұнда CRAMM бірнеше қарсы әрекет шараларының нұсқасын адекватты түрде шығарылған қатерлер мен олардың деңгейлеріне түрлендіріледі.

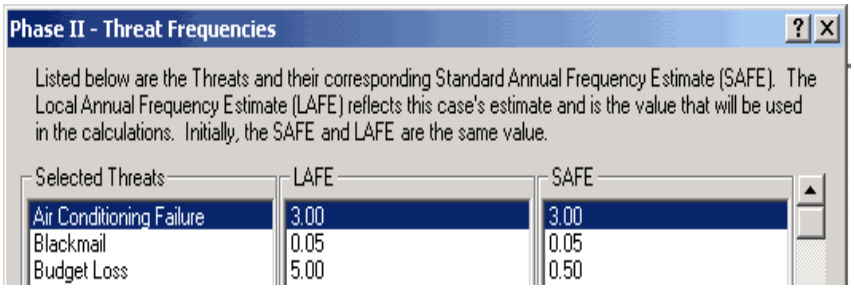
Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Сурет. 1.3 - Қатер бағасының матрицасы

Барлық кезеңдерді өткеннен кейін нәтижеде ақпараттық жүйе толық сипаттамаға ие. Қауіп-қатермен әлсіздіктер бағасы қатердің бағалануы негізінде екі фактор бойынша жүзеге асады: қатер әлсіздік пен қауіп-қатерді, сонымен бірге зиянды жүзеге асыру ықтималдығы түрінде қарастырылады [1,12]. Қауіп-қатер мен әлсіздікті бағалау процесінде барлық баллдардың жалпы саны шығарылады да, анықталған диапазонға қатысты, оннан шыққан мән олардың дәрежесін бейнелейді. Мысалы, егер қауіп-қатердің балл қосындысы 25-ке тең келсе, онда ол орташа мән түрінде қаралады да, қауіп-қатер дәрежесі үшін қолданылып жатқан шкала мынадай болады: 9 балға дейін – өте төмен; 20 дан 29-ға дейін – орташа; 40-тан аса – өте жоғары. Осыған сәйкес әлсіздерге де мысалы, егер баллдар қосынды 53-ке тең болса, онда ол жоғары деп бағаланады да, әлсіздікке арналған шкала мынадай болады: 9 балға дейін – төмен; 20-дан астам – жоғары. Бұл әдістеме қазіргі күні бар болған жүйелерге сай келеді де, оларды өңдеу кезінде жарамсыз, себебі, қатерді сапалы бағалау үшін АЖ-нің толық сипаттамасы қажет болады.

ҚБАҚ 3 - RiskWatch (RiskWatch - АҚШ өңдеуші компаниясы) **жүйесі** ISO/IEC 27001 және ISO/IEC 27002, NIST стандарттар талабын, сонымен бірге, COBIT IV сипаттайды. Қатерді бағалау мен анализдеу процесі төрт фаза арқылы өндіріледі. 1-Фаза – Ақпараттық қауіпсіздік көзқарасы тұрғысынан АЖ ұйымының сипаттамасы (зерттеудің пәндік аймағының анықталуы). Мұнда кәсіпорынның мынадай параметрлері сипатталады: ұйымның типі, зерттеліп жатқан жүйенің құрамы, Ақпараттық қауіпсіздік саласында бастапқы талаптар. Жұмысты жеңілдету үшін аналитикада іріктірілген тізімдер (қорғаушы категориялар тізімі: ресурстар, шығын, қауіп-қатер мен қорғау шаралары)

қолданылады, олардың әрқайсысында ұйымда нақты бар құраушыларды таңдауды жүзеге асыру мүмкіндігі бар, мысалы, шығын категориясында мыналар болуы мүмкін: қызмет көрсетуде іркілу және бас тарту, ақпараттың ашылуы, тікелей шығындар (мысалы, өрт кезінде құрал-жабдықтардың жойылуынан), жанама шығын (мысалы, қайта құруға кеткен шығындар), өмір мен денсаулық (қызметкерлердің, тапсырыс берушілердің т.т.б.), мәліметтердің, абырой-беделдің өзгеруі [8] т.б. 2-Фаза – мәліметтерді енгізу. Әлсіздіктерді анықтау үшін тақырыптық сауалнама (ТС) инициализацияландырылады, оның қоры 600-ден астам сұрақтардан құралған. Анықталған әрбір қауіп-қатерге, әлсіздік дәрежесіне және ресурстардың (белсенділердің) құндылығына жиілік беріледі де (1.4 - суреті), осының негізінде АҚор құралдарын енгізудің тиімділігі есептеледі [9].



Сурет 1.4 - Параметрлердің инициализациялау терезесі

RiskWatch-гі (мәліметтерді өңдеу мен енгізуді жеңілдету үшін) COBRA ПҚ-дың аналогиясы бойынша ТС-дағы көптеген сұраныстар нұсқасын теруден мәліметтерді таңдау арқылы инициализацияландырылады, мысалы, нақта сандар мәні (0, 1 – «ешқашан», 2, 3 – «сирек», 4, 5, 6 – «анда-санда»; 7,8 – «әдетте»; 9, 10 – «әрқашан») немесе «жоқ», «білмеймін». Сұраныстар арқылы Ақпараттық қауіпсіздік-тің кезектегі ережелері бар болған стандартқа сәйкес бағаланады, әрі көрінеді. RiskWatch-тағы сұранысқа, мысалы, «ерекше компьютерлер мен файлдық серверлерге, нүкте мүмкіндігіне, ішкі және сыртқы жүйеге қол жеткізуде шектеу бар ма?» - болуы мүмкін. 3-Фаза – қатер бағасы. Қатер профилі есептеледі және Ақпараттық қауіпсіздік қамтамасыздандыру шаралары таңдалады. Ол үшін алдында анықталған ресурстар, шығындар, қауіп-қатерлер мен әлсіздіктер арасында байланыс орнатылады, ал қатер бір жылда күтілетін шығындар арқылы бағаланады. Мысалы, егер сервер бағасы $v = 150000\$$, ал өрт кезінде оның бір жыл ішінде жойылу ықтималдығы p=0,01 болса, онда күтілетін шығын $m = 1500\$$, яғни $m = p \times v$ құрайды, мұндағы p – қауіп-қатердің пайда болу ықтималдығы, ал v – ресурс бағасы. Айта кететін жайттардың бірі, бұл, RiskWatch SAFE (Standard Annual Frequency Estimate) және LAFE (Local Annual Frequency Estimate) сияқты NIST мәліметтеріне негізделеді, сәйкесінше жергіліктенген (мысалы, қалада), әлемдескен (мысалы, Солтүстік Америкада) салаларда қауіп-қатердің жүзеге асуының жылдық жиілігін сипаттайды. Ресурсты біртіндеп жоятын түзеуші коэффицентте қолданылады. LAFE және SAFE бағаларын алу, мысалы, Украина үшін

проблема болып табылады, себебі, қажетті статистика жоқ. Мысалға, АҚШ-да инциденттер (The Uniform Crime Reporting) туралы мәліметтерді жинайтын ұлттық программа бар, бұл өз кезегінде жалпы мемлекеттік қорда АҚ-дың инциденттері туралы бар болған статистикалық ақпаратты қалыптастыруға мүмкіндік береді. 4-Фаза – есептің түрленуі (1.5-сурет). Стандарт талабына сәйкестігі мен сәйкес келмеуі (сұранысқа байланысты) детальді елестету кестесі мен диаграммасы, сонымен бірге шығын диаграммасы қалыптасады. Ресурстың бағасына байланысты бір қауіп-қатердің жүзеге асуынан күтілетін шығынның (нақты белгілі белсенді бойынша) бағасы жүзеге асырылады, (*ALE*) [12] $ALE = A \times EF \times F$, мұндағы: *A* (Asset Val) – ресурс бағасы (мәліметтер, программалар, аппараттар т.б.); *EF* (Exposure Factor) – әсер ету коэффициенті (қатерге душар болып жатқан белсенді бағасының пайыздық бөлігі); *F* (Frequency) – жағымсыз оқиғаның пайда болу жиілігі. Мысалы, аппараттық құрал *A*=10000$ тұра қойсын, оған әсер ету коэффициенті де *EF*=0,5 болсын, ал жиілік *F*=0,2 болса, онда күтілетін шығындар *AEL*=1000$ құрайды. Белсенділер мен әсер етулер идентификациясынан кейін АЖ үшін жалпы қатер бағаланады (барлық жеке мәндер қосындысы).

Theft - Company Property - AFE: 2.00

The various incident classes associated with this threat are shown in the following table:

Incident Class	SLE	ALE	% of total ALE
Delays/Denials, Communications Equipment	$26,401.	$52,801.	68.0%
Delays/Denials, Data/Information	$4,400.	$8,800.	11.3%
Delays/Denials, Physical Inventory/Product	$2,750.	$5,500.	7.1%
Direct Loss, Cash	$2,200.	$4,400.	5.7%
Delays/Denials, Production Resources	$1,100.	$2,200.	2.8%
Direct Loss, Physical Inventory/Product	$1,100.	$2,200.	2.8%
Direct Loss, Data/Information	$550.	$1,100.	1.4%
Direct Loss, Production Resources	$275.	$550.	0.7%
Direct Loss, Communications Equipment	$39.	$77.	0.1%

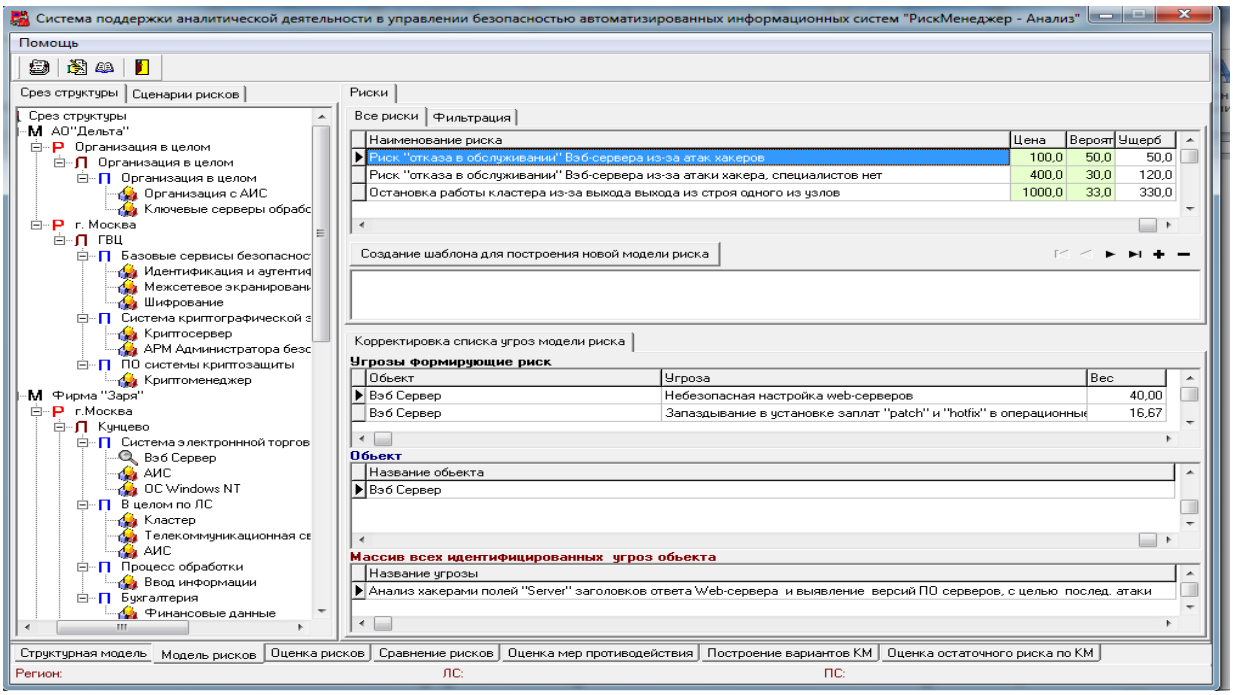
Сурет 1.5 - RiskWatch есебінің көрінісі

Қосымша түрде ARO (Annualized Rate of Occurrence) – күтілетін уақиғаның жылдық жиілігі мен SLE (Single Loss Expectancy) – күтілетін жеке-дара зиян (белсенді бағасының бастапқы және қалдықтық айырмашылығы (уақиғадан кейінгі)) көрсеткіштері қолданылады. Бөлек алынған «қауіп-қатер-ресурс» жұбын бағалау үшін $ALE = ARO \times SLE$ формуласы қолданылады. Сонымен бірге, қорғау құралдарын енгізу шарттылығы кезінде ұқсас жағдайларды сипаттауға көмек беретін «что, если:» сценариі де қолданылады. Қорғаныс шараларын енгізу шарттылығы кезінде, және де оларсыз да күтілетін шығындарды салыстыра отырып, мұндай шаралардың нәтижесін бағалауға болады. Бұл үшін RiskWatch-та тек LAFE және SAFE мәліметтер қоры ғана емес, сонымен бірге

әр түрлі ақпаратты қорғау жүйесінің (АҚЖ) қоры бар. қауіпсіздік құралдарын енгізудің нәтижесін уақыт аралығындағы салынған қаржыдан қайтарып бергенді көрсететін *ROI* (Return on Investment – инвестицияның қайтарылуы) параметрі арқылы анықтауға болады.

ҚБАҚ 4-RA2 art of risk (RA Software Tool, Ұлыбритания өңдеуші –AEXIS Security Consultants және XiSEC Consultants Ltd. компаниялары) **аспабы** ақпараттық қауіпсіздіктің менеджмент жүйесін (АҚМЖ) ISO/IEC 27001:2005 талабына сәйкес жүзеге асыру үшін ПҚам болып табылады. Сегіз модульден тұрады: АҚМЖ саласы мен қатер бағасының көлемі; белсенділер идентификациясы; белсенділер бағасы; қауіп-қатер/әлсіздіктер бағасы; қатердің бағасы мен идентификациясы; қатерді өңдеу бойынша шешімдер; қабылданып жатқан шараларды бекіту; шаралардың орындалуы мен басқару құралдарын сараптау. әр бір модульді орындау процесінде сұраныстардың инициализациясы бинарлық-лингвистикалық («иә», «жоқ») формада шектелген мәнді таңдау арқылы жүргізіледі. Қатерді бағалау үшін сегіз деңгей қолданылады: 1 – тривиалды; 2, 3 – минорлы; 4, 5 – мәнді; 6, 7 – үлкен; 8 – апаттық, ал қатер матрицасы кәсіпорын қатерінің деңгейі және лингвистикалық шкалаларда қатер ықтималдығын егізінде құрылады. қатер мәні әрбір ұсынылған категориялар бойынша лингвистикалық және цифрлық деңгей түрінде қалыптасады, мысалы, «жоғары деңгей» мәніне 7 саны сәйкес келеді [8].

ҚБАҚ 5-«АванГард» Ақпараттық қауіпсіздік басқармасының КСЖ жүйесі («АванГард» комплексті сарапшылық жүйесі, Ресей өңдеуші – РҒА жүйелі анализдеу Институтын ақпараттандыру мәселелерін анализдеу лабораториясы) әдістемелер кешенін кіргізеді: автоматизацияланған АЖ-нің (ААЖ) Ақпараттық қауіпсіздік-нің бұзылуын БАҚ негізінде өте маңызды ақпараттық инфрақұрылым объекттері мен сегменттерін идентификациялау; үлкен компьютерленген жүйе ұйымдарының Ақпараттық қауіпсіздік бұзылу қатерін басқару; ААЖ өте маңызды объекттері мен сегменттерін Ақпараттық қауіпсіздік талап жүйесінің құрылуы; ААЖ өте маңызды объекттері мен сегменттерінің жағдайы үстінен мониторингтік бақылау. Жүйе екі программалық кешенге негізделеді – «АванГард-Анализ» және «АванГард-Бақылау» [64]. Қатер оқиғасының ($\boldsymbol{BC_1}$) анализі олардың моделін интерфейстің басты формасы көмегімен құру арқылы алдын ала жасалады (1.6 суретінде), мұндағы жоғарғы секторда қатер оқиғаларының модельдер тізімі кестеде берілген, олардың әрбір графасында оның оқиғасының ықтималдылық (пайыз түрінде) пен қатер құнының (шартты бірлікте) сарапшылық бағасы берілген.

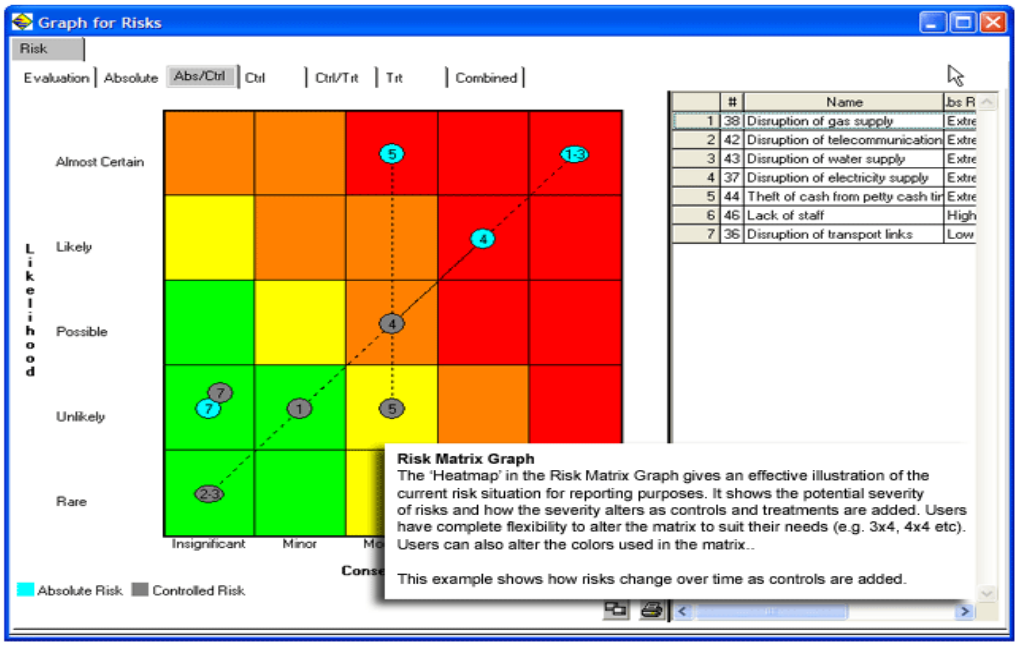


Сурет 1.6 - Қатер оқиғасының моделін құру интерфейсі

Шартты бірліктегі материалды зақымдануда бағалы эквивалентті меншіктеу ұсынылады, мысалы, 1000 руб. Қатер оқиғасы кезінде, қаржылай бағалауда қиындыққа соғатын зақымдануда, олардың қауіп дәрежесіне қарай қатер оқиғасы сараланатын баллды бағалау қолданылады. «Зақым» графасында қатердің айыру мәні оның бағасы мен ықтималдығына қарай идентификацияланады. Келесі секторда қауіп-қатердің кестесі берілген, олардың жүзеге асуы қатер оқиғасына алып келуі мүмкін. Әрбір қауіп-қатерге алдын-ала берілген оқиға салмағы көрсетіледі (қатер оқиғасы бойынша қауіп-қатердің қатер туғызушы потенциалы (ҚТП)). Баға үшін қажетті: қатерге алып келетін әрекет сипаттамасымен объект класын таңдау (оның идентификаторын анықтау); әрбір қатер үшін қаржы эквивалентін құру; осы қауіп-қатерді жүзеге келтіру нәтижесінде пайда болуы мүмкін болған қатер оқиғасын (нормативті модель құрамына кіретін қауіп-қатер мәнділігін анықтау үшін) қарастыру. Әдетте, әрбір оқиға қауіп-қатердің кейбір жиынтығының жүзеге асу нәтижесі. Бұл, бір оқиғаны анализ жасау жолымен қауіп-қатердің бір емес, бірнешеуінің маңыздылығын анықтауға мүмкіндік береді. Берілген жүйеде қатер оқиғасының моделі деп аталатын қатер, қауіп-қатер тізімі, оқиғаның ықтималдылық бағалануы, қатер бағасы, сонымен қатар, берілген бағаларды аналитикалық негіздеу оқиғасының сипаттық жиынтығынан тұрады. Ол оқиға сарапшысының көзқарасы бойынша әр бір мүмкін болғанда құрылады [64].

ҚБАҚ 6-Enterprise Risk Assessor (Risk Advisor, Жаңа Зеландия өңдеуші–Methodware компаниясы) **жүйесі** ISO/IEC 17799 және Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) австралиялық стандарт талабына сәйкес келеді. Үш өнімде берілген: CobiT Advisor 3rd Edition (Audit); PRo Audit Advisor; Planning Advisor. БАҚ процесі үш қадам арқылы қосылып, ол бағаны

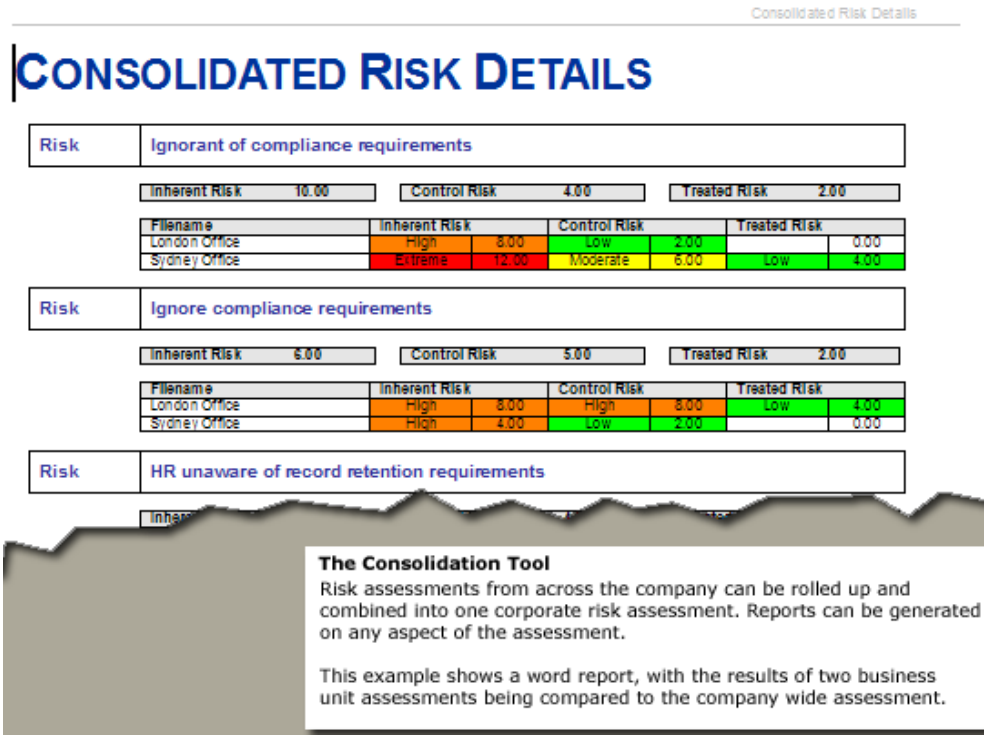
құрастыруға, оны дәлірек етуге мүмкіндік береді. 1-қадам: The Builder Tool үстемесі – аудит (ақпаратты жинау) пен қатер баға құрылымын жасауға арналған аспап. Функционалдық мүмкіндіктерінің кез келген бөлігін қосатын немесе жасыратын қабілеттігін қоса, ол АЖ құрылымын құруға да мүмкіндік береді. Бұл үстемедегі жұмыстың негізгі кезеңі АЖ, қатерлер, қауіп-қатерлер, шығындар мен анализ шешімдерінің сипаттамасынан тұрады. «Қатер сипаттамасы» кезеңінде белгілі бір үлгіге сай қатерлерді сипаттауға және модельдің өзге элементтерімен олардың байланысын жасауға мүмкіндік беретін матрица жасалады (1.7 сурет). Баға сапалы шкала негізінде жасалады, ал қабылданарлық және қабылданбайтын болып бөлінеді.



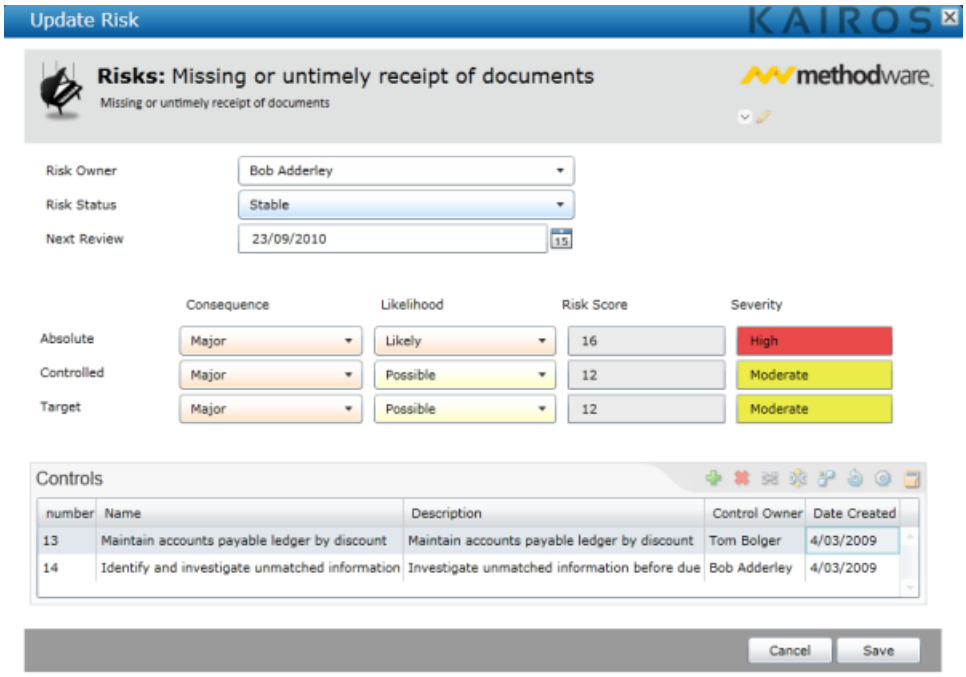
Сурет 1.7 - Қатер матрицасы

Әрі қарай басқару ықпалдары (контршаралар) алдын ала белгіленген жүйе критериесін, контршара тиімділігі мен олардың бағасын есепке алғанда таңдалады. Сонымен бірге құны мен тиімділігі сапалы шкалаларда бағаланады. «Қауіп-қатер сипаттамасы» кезеңінде қауіп-қатер тізімі баста қалыптасады, оларды классификациялау жүзеге асырылады, қатермен байланысы сипатталады. Сонымен бірге сипаттама да сапалы деңгейде жасалады, бұл олардың байланысын белгілеп алуға мүмкіндік береді. «Шығынды сипаттау» кезеңінде АҚ тәтібінің бұзылуымен байланысты болған оқиғалар сипатталады. Шығындар таңдалған критериилер жүйесінде бағаланады. Мәліметтерді жинауды жеңілдету үшін сарапшылар қолдан жинайтын ТС-ді қолданады. Ақпаратты жинап болған соң қатерді бағалауға кірісеміз. 2-қадам: The Assessor – сарапшылық бағалау (жиналған ақпаратты талдау). 3-қадам: The Consolidation Tool – аспаптардың бірігуі (қатердің барлық жеке бағаларын интеграциялайды). Модель құрылғаннан кейін есеп (100-ден астам бөлімді) пен қатер графасы түріндегі біріктірілген сипатама қалыптасады [55, 65]. лингвистикалы-

ықтималды шкаласы бар есепте (1.8. суретте) қатер градациялы матрица түрінде берілген: қалайда дерлік, бәлкім, мүмкін, екіталай, сирек. қатерді бағалау мен сипаттау үлгісін қарастырайық (1.9 суретте). Сипаттау процесінде сарапшы иесі мен қатер дәрежесі, салдар мен ықтималдылық көрсетіледі, әрі қарай бағалау жүзеге асырылады.

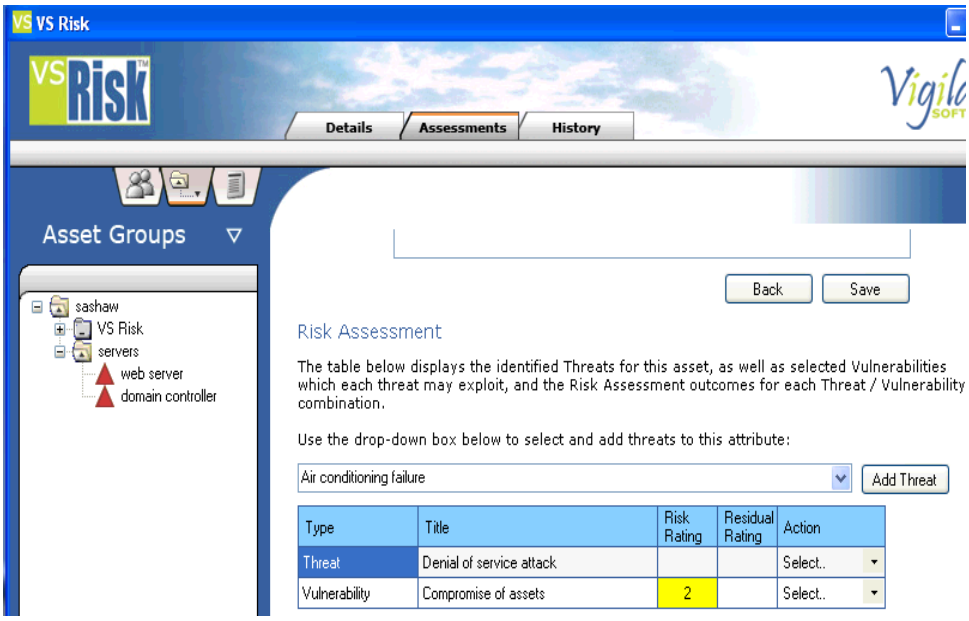


Сурет 1.8 - Есеп көрінісі



Сурет 1.9 - Қатерді сипаттау үлгісі

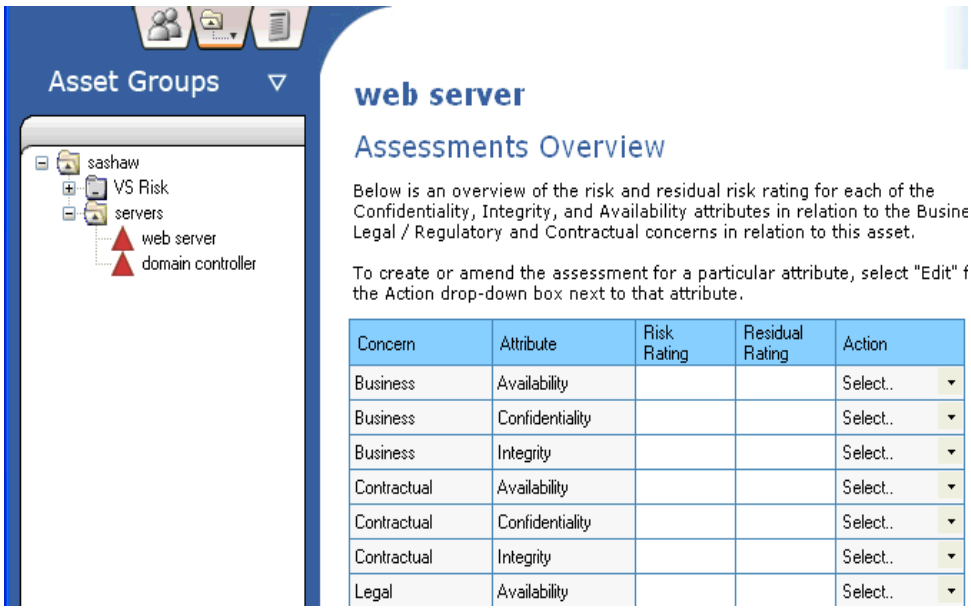
ҚБАҚ 7-vsRisk, Risk Assessment Tool (Ұлыбритания өндеуші – Vigilant Software Ltd. компаниясы) **жүйесі** АҚ қатерін ISO/IEC 27001 және BS 7799-3 талабына сәйкес бағалауға арналған. Қатерді бағалау процесін жеңілдету үшін әсер ету мен ықтималдылық шкалалары (деңгейлер орнықтырылады) таңдалған визардтар қолданылады. Әрі қарай әрбір әрекет, мысалы, «Қызмет көрсетуден бас тарту» таңдалған шкалалар бойынша ықтималдылық анықталады (1.10 суреті).



Сурет 1.10 - Қатер бағасы интерфейсінің үлгісі

Жүйе қауіп-қатерді, әлсіздікті, белсенділер мен бақылау механизмдерін қоса қатерлер факторларның барлық бағалары үшін құралдарды ұсынады да, қатер көлемін санды бағалауға арналған құралдардан тұрмайды, тек сапалы шкалалармен шектеледі. Айта кететін жайт, бағалау үшін қаралатын қауіп-қатер әсер етуі мен ықтималдық масштабы беріледі. Жұмыс барысы бойынша өнімнің мәліметтер қорына енетін барлық өзгерістер егжей-тегжейлі аудит журналында тіркеледі.

Қатер анализінен соң ықтималдылық үшін таңдалған балл түрінде баға беріледі, мысалы, 1.11. Бағалардың нәтижесі бойынша «Бақылаудың қолдану механизмі туралы декларациясы» және «Қатерлерді өңдеу жоспары» ISO/IEC 27001 стандартының талабына сәйкесінше қалыптастырылады. Әрі қарай бұл ақпарат осы стандартқа сәйкестену ұсынысын қорытындылау кезінде қолданылады. vsRisk-те ұсынылған әрекеттердің әрі қарай сипаттамасы бар қатерді бағалау детальді түрде жоқ (1.11. сурет) [9, 66].



Сурет 1.11 - Бағалардың қысқаша көрінісі

1.3 Ақпараттық қауіпсіздік қатерін бағалаудың аспаптық құралдары

ҚБАҚ 8-OCTAVE (Carnegie Mellon Software Engineering Institute және Білім беру-АҚШ өңдеуші институты, (CERT) технология мен зерттеу орталығы өнімдер тізімінде жүзеге асырылады: сәйкесіншеірі, орташа және кіші ұйымдар үшін –OCTAVE, OCTAVE-S және OCTAVE Allegro әдістері) **жүйесі**, ұйымдық және техникалық сұрақтарды үйрену үшін үш кезеңді тәсілді қолданады. 1-Кезең – «әлсіздіктер мен белсенділер идентификациясы», бұл үш процесстен тұрады: «Басқарудың ресурстар идентификациясы» (комания өкілі тарапынан әр түрлі белсенділер, ақпараттық қауіпсіздік талаптары, қауіп-қатер мен әсер етуі туралы ақпараттар жиналады); «Эксплуатациялық ресурстардың идентификациясы» (алдынғы процестегі сияқты сарапталған эксплуатациялық салалардан ақпарат жиналады); «Штат ресурсының идентификациясы» (алдыңғы процестерге ұқсас жалпы штаттардар сарапталған эксплуатациялық салалардан ақпарат жиналады); «Қауіп-қатер пішінін жасау» (қауіп-қатер пішіні сын ресурстардың 3 ÷ 5 таңдалуы үшін анықталады). Бұл кезеңді өту үшін жүйеде ТС-ны инициализациялау ұсынылады (1.12 сурет).

Container Type	Questions to Consider
Technical (*see* **Worksheet 9a**)	*Internal* ❑ What information systems use or process this information asset? *Example:* • *The vendor database (information asset) is used by the accounts payable system (system).* ❑ What automated processes are reliant on this information asset? *Example:* • *Paying an invoice (process) requires information in the vendor database (information asset) and is automated in the accounts payable system (system).* ❑ On what hardware might this information asset be found? Consider: • If the information asset is used by a system, application, or process, what underlying hardware is related to the information asset? *Examples:* • *The vendor database is stored on the "DIAMOND" server.* *External*

Сурет 1.12 – 1-ші кезең үшін сұраныс үлгісі

2-Кезең – «Инфрақұрылымның әлсіздіктері мен қауіп-қатерінің идентификациясы» екіпроцестен тұрады: «кілттік компоненттер идентификациясы» (жүйенің кілтті компоненттерінің толымды жиынтығы құрылады, бұлар сын ақпараттар-байланыс белсенділерін өңдейді немесе қолдайды); «Сарапталған компоненттер бағасы» (шешімдер анализі мен сарапталған компоненттер бағалауы жүргізіледі). Қауіп-қатерді келесі категорияларға бөледі: адамның қатысуымен және техникалық құралдарды қолданумен; адамның қатысуымен және физикалық мүмкіндіктері қолданумен; техникалық проблемалар; өзге проблемалар. 2-кезеңге өту кезінде қатер $R(T, I)$ функциясы түрінде анықталып, мұндағы T – қауіп-қатер (threat)/шарттылық (condition), ал I – әсер ету (impact)/салдар (consequence). Сонымен бірге қатер басталған жағдайда компанияға төнетін қауіп-қатер детальді түрде сипатталады. Қауіп-қатер (шарттылық) сценариінің үлгісін қарастырайық – мүмкіндіктің шектелу саясатының дұрыс еместігі қызметкердің кездейсоқ түрде өзге қызметкерің медициналық жазбаларына қол жеткізу мүмкіндігін береді; әсер ету (салдар) – қызметкердің медициналық жазбасы оның қуыным беру нәтижесінде ашылады да, ұйым 50000$ көлемінде айып пұл төлеуге міндетті болады. Бұл қауіп-қатер кәсіпорынның беделіне тікелей әсер етеді, бұл өз кезегінде потенциалды қаржылай шығындарға алып келеді (соттық қуыным, мүмкін болған айып пұл, пеня т.б.). 3-кезең – «Қауіпсіздік жоспары мен стратегияларының дамуы» (ұйымның сыншы белсенділеріне қатерлер идентификацияланады және оларды өңдеу бойынша шешімдер қабылданады) екі процестен тұрады: «Қатерді бағалау мен анализдеу» (сыншы белсенділерге қауіп-қатердің әсер ету дәрежесі (жоғары, орташа, төмен) анықталады; «Қорғау стратегиясының дамуы» (команда барлық ұйымның қорғаныс стратегиясын оның ақпараттық қауіпсіздік қамтамасыздандыру әдістерінің жақсаруын көздей

отырып дамытады [56]). Көрсетілген мысалды қолдана отырып (медициналық жазбалар туралы) берілген қатер әрекетінің аясы бойынша бағалау процесін қарастырайық (мұнда шкалалар қолданылады – орташа, төмен, жоғары) (1.2-кестесі).

Кесте 1.2 - Қатерді бағалау процесінің үлгісі

Қатер әрекетінің аясы	Қатер деңгейі
Атақ-беделі/клиенттер сенімі	Орташа
Қаржылар	Төмен
Өнімділігі	Төмен
Денсаулығы мен қауіпсіздігі	Төмен
Айып пұлдар	Жоғары

Келесі жалпы бағалу кезінде әрбір аялары үшін қатер деңгейінің коэффициенті беріледі: жоғарғы – 3, орташа – 2, төменгі – 1. Қатерді бағалау процесінде әрбір қауіп-қатер бойынша алынған баллдар жинақталады (1.13 сурет).

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	**8**
Financial	5	Low (1)	**5**
Productivity	3	Low (1)	**3**
Safety and Health	1	Low (1)	**1**
Fines/Legal	2	High (3)	**6**
		Total Score	**23**

Сурет 1.13 - Жалпы қатер бағасының нәтижесі

ҚБАҚ 9 - Callio Secura 17799 (Канадаөңдеуші – Callio Technologies компаниясы) **аспабы** ISO/IEC17799/BS7799 стандарт талабына сай АҚМЖ-нің сертификаттауы, басқаруы, енгізуі, өңдеуі кезінде менеджер үшін қажеттінің бәрін қосатын web-үстеме болып табылады [67]. Жүйе төрт секциядан тұрады: «Әдіснама» – BS7799-2 сертификаттауына өту мен ISO/IEC17799 енгізуді дұрыс жүзеге асыру қадамдарын түсіндіруші көмекші; «Әкімшілік ету» – АҚМЖ-нің басқарма құрылымын дұрыс анықтауға арналған аспап; «Аспаптар» – ISO/IEC17799 талаптарын дұрыс орындауды жүзеге асыруға арналған аспаптар жиынтығы; «ақпараттық қауіпсіздік басқару» – АҚМЖ-нің аудитіне тиімді дайындалуға және қатерлерді ұйымдастыруларды тиімді басқаруға мүмкіндік беретін модульдер. Ақпараттық қауіпсіздік қатерін бағалау үшін стандарт талаптарына сәйке құрылған ТС инициализациялау қажет. ТС-дағы сұраныс үлгісін қарастырайық: «Барлық қызметкерлер хабарландырылған және

баспаға түскен құжаттанған (бекітілген) саясатшылар бар ма?». Қатерді бағалау мен анализдеу процесі екі кезеңнен өтеді, біріншісінде – қол жетімділіктің, тұтастықтың, құпиялылықтың бұзылуы нәтижесінде шығынмен анықталатын белсенділер, қауіп-қатерлер, әлсіздіктер мен Ақпараттық қауіпсіздік талаптарының идентификациясы жүргізіледі, әлсіздіктер, қауіп-қатер ықтималдығының және белсенділер құндылығының көлемі бағаланады. Осы мәліметтерді қолданудың арқылы қатер мәні есептеледі. Екінші кезеңде қатерді өңдеу амалдарына және қалдық қатерлердің қабылданарлық деңгейіне қатысты шешім қабылданады, қатерді өңдеу жоспары жасалады, ақпараттық қауіпсіздік саясатын және басқа да ұйымдастырушы-басқарушы құжаттарды өңдеу мен бақылау механизмдерінің енгізілуі жүргізіледі. Сипаттау кезінде критерийге қатысты мәліметтерді беру қажет «жоғарғы» – (3), «орташа» – (2), «төмен» – (1) [67] (1.14 суреті). Қауіп-қатер ықтималдығы мен белсенділердің құндылығы туралы ақпаратқа негізделе отырып, қатер мәндері автоматты түрде есептеледі де, басымдылықтар (құпиялылық, тұтастық, қол жетімділік және заңдылыққа байланысты қатер) бойынша реттестіру жүргізіледі.

Сурет 1.14 - Қатер бағасының үлгісі

ҚБАҚ 10 - Гриф 2006 (Digital Security – Ресей өндеуші компаниясы) **жүйесі** компания қауіпсіздігін қамтамасыздандыру бойынша бар болған практиканың тиімділігі мен АЖ-гі қатер деңгейін бағалау бойынша (өзге сарапшылардың қатысуынсыз), АТ-менеджментінің өз бетінше жұмысын қамтамасыздандыруға бағытталған сонымен бірге ақпараттық қауіпсіздік саласына инвестицияның қажеттігін басқармаға дәлелді түрде (санды түрде) сендіру мүмкіндігін ұсынады. Гриф 2006-да қатерді бағалау процесі үш кезеңнен тұрады. 1-кезең – ақпараттық ағындардың анализ (компания белсенділерінің және барлық бизнес-процестерінің сипаттамасы). 2-кезең –

әлсіздіктер мен қауіп-қатерлер анализінің моделін жасау. Бағалау үшін өңделген Digital Security қауіп-қатер классификациясы қолданылады, мұнда бағалау кезінде ақпараттық қауіпсіздік сипаттама қорының бұзылуына яғни ақпараттық қауіпсіздік бұзылуының оқиғаларына алып келуі мүмкін барлық әрекеттер сипатталды. 3-кезең – құнды ресурстардың әрқайсысына барлық қауіп-қатер түрі бойынша зақымдануын көрсету. Бұл жүйеде жүзеге асырылған ақпараттық қауіпсіздік саясаты бойынша ТС-ны инициализациялау қажет, бұл қатер бағасын детальдастыруға және оның нақты қорғану деңгейін бағалауға мүмкіндік береді. ТС-да сұраныстар (мысалы: «Қандайда бір ақпараттың ашылуы қызығушылық танытқан ұйымдарға өзге тұлғаларға т.б. айтарлықтай пайда алып келуі мүмкін бе?») тіркелген екі нұсқаның бірімен инициализацияланады – «иә» немесе «жоқ». Ақпараттық қауіпсіздік қатерлер анализі ұйымның АЖ-нің моделін құру арқылы жүзеге асырылады [62]. Қатер бөлек әрбір байланыс арқылы «тұтынушылар тобы – ақпарат» бағаланады, яғни модель өзара байланысты оның барлық сипаттамасын есепке ала отырып «субъект – объект» қарастырады. Қауіп-қатердің жүзеге асу ықтималдығы, оның әлсіздік бойынша деңгейі мүмкін болған зақымдануы және берілген әлсіздік арқылы жүзеге асу ықтималдығы мен сынының негізінде есептеледі. Жүйеде 0- ден 100% дейінгі шкаласы қолданылады.

ҚБАҚ 11 - @RISK (Palisade өңдеуші компаниясы АҚШ) **жүйесі** Microsoft Excel негізінде жүзеге асушы Монте-Карло әдісінің көмегі қатерді бағалауға арналған. Жүйе қатерді қабылдау мен қашу мүмкіндіктерін бақылауға, сонымен бірге белгісіздік шарттылығында тиімдірек шешімдер қабылдауға мүмкіндік береді. Жүйеде әртүрлі сұраныстар қалыптасады, мысалы, «10 млн. доллардан асатын пайда ықтималдығы қандай?» немесе «Осы кәсіпорында ақшаға шығындалу ықтималдығы қандай?». Қатерді бағалау үшін Value at Risk (VAR) әдісі де қолданылады [68]. Жұмыстың бастапқы кезеңінде кестені толтыру арқылы (қатер анализін) бағалау моделін жасау жүзеге асырылады (1.3 кестесінің үлгісін қара).

Кесте - 1.3 Эксплуатациялық қатерлеркестесінің үлгісі

Эксплуатациялық қатерлер	Ықтималдылық (жылдық) %	Әсер ету ($)	Орташа әсер ету ($)
1	2	3	4
IT жүйенің істен шығуы	0,1	1000	5
Өндірістік процесспен проблема	0,05	50	3
Басқару мүшесінің ауыр сырқаттануы	0,05	100	5
Қызметкер сот процесін жеңіп алуы	0,08	250	20

1	2	3	4
Жаңа басекелестің пайда болуы	0,25	400	100
Жаңа тауарды шығарудан бас тарту	0,15	300	45
Бағамның тұрақтануы $	0,35	100	35
Бас кеңседегі өрт	0,02	250	5
Алаяқтық	0,005	500	3
Құпиялы мәліметтердің жоғауы	0,01	300	3
Қарыздар басты клиенттің банкроттануы	0,02	150	3
Жалпы саны		2900	226

Егер ақпараттық қауіпсіздіктің бұзылу жағдайы болса, әрі қарай шығындардың есептелуі жүзеге асады.

ҚБАҚ 12 - RiskPAC (CSCI-өңдеуші компаниясы, Нидерланд) **жүйесі** АЖ-гі әлсіздіктерді жою кезіндегі көмек көрсету мен табуға арналған. Анкета конструкторы кез келген қатерді қолмен бағалау әдісін автоматизациялауға мүмкіндік береді, оны анализдеу үшін мәліметтер қорында реляция түрінде берілген ТС-ғы сұранысты (тіркелген нұсқалар көмегімен) инициализациялау қажет. Әрбір сұраныс ақпараттық қауіпсіздіктің бұзылуына алып келетін белгілі бір әрекетті бейнелейді. Сұраныс үлгісін қарастырайық: «Клиенттік қор тұтастығының бұзылуы кезінде бір тәуліктегі қаражаттық шығын қандай болады?». Қатерлерді бағалау кезінде қауіп-қатер ықтималдылығын есептеу үшін шкала қолданылады: екіталай, ықтималды және ең ықтималды. Сонымен бірге әсер ету де шкала бойынша есептеледі: минималды, айтарлықтай, маңызды және апаттық. Жүйе қосымша түрде күтілетін орташа жылдық шығын есептеу калькуляторынан тұрады.

ҚБАҚ 13 - Microsoft Security Assessment Tool (MSAT, Microsoft - АҚШ өңдеуші компаниясы) **жүйесі** «Қатерлерді басқару бойынша жетекшілік» материалдарына негізделеді [47]) келесі функцияларды орындайды: 1) қатерлерді бағалау; 2) шешімдерді түсінуді қолдау; 3) бақылауды жүзеге асыру; 4) программа тиімділігінің бағасы. Үстеме ақпараттық қауіпсіздік саласындағы потенциалды мәселені бірлесіп жақсы түсінуде 1000 адамнан астам қызметкерлерді ұйымдастыруға бағдарланған. Жұмыс барысында ақпараттық қауіпсіздік сұрақтарына жауапты аналитик ролін атқаратын тұтынушы сұраныстардың екі тобымен жұмыс істейді. Оның біріншісі, компания бұл саламен таңдаған бизнес-модель шарттылығында соқтығысатын бизнес үшін қатерді бағалауға арналған. Бизнес үшін, өзгеше айтқанда, қатер келбеті жасалады. Бұл топ сұранысы 6 кезеңге бөлінген: 1-кезең – «Компания параметрлері» (атауы, серверлер, компьютерлер саны т.б.); 2-кезең – «Инфрақұрылым қауіпсіздігі» (бұл кезең үшін сұраныстар үлгілерін қастырайық: «Ішкі және сыртқы клиенттермен қолданылатын қызметтер сол бір сегментте орналастырылады ма?», «Клиенттің үстемесіне немесе инфрақұрылымына зиян алып келетін, мысалы, орталықтың әрекетсіздігі, құрал-жабдықтың істен шығуы немесе үстеменің шалыс соғылуы т.б., оқиғаның табыстылығына әсер ете ма?); 3-кезең – «Үстемелердің қауіпсіздігі»; 4-кезең –

«Операцияның қауіпсіздігі»; 5-кезең – «Қызметкерлердің қауіпсіздігі»; 6-кезең – «Орта». Осы топтардың кезеңдерін жүзеге асырған соң алынған ақпаратты (Ғаламторға қосылу арқылы) өңдеу жүзеге асырады да, сұраныстардың екінші тобына өту жүзеге асырылады. Техникалық мамандар үшін бұл өте қызықты, себебі бұл компанияда қолданушы саясатшылар мен құралдарға және ақпараттық қауіпсіздік механизмдеріне қатысты. Сұраныстар АҚор-дың көп деңгейлі (эшелондап орналастырылған) концепциясына сай ұйымдастырылған деңгейі: қызметкерлермен жұмыс істеу (жұмысқа қабылдау кезінде тексеру, оқыту т.б.); операцияның қауіпсіздік (қор көшірмесінің саясаты, ақпараттық қауіпсіздік саясаты т.б. анықталған ба); инфрақұрылымдар (периметрдің, аутентификациялар т.б қорғау); үстемелер. ТС көбіне ISO/IEC 17799 және ISO/IEC 27001 стандарттар бөлімдеріне сәйкес келеді. Сұраныстарды инициализациялаудан кейін программалық жүйенің клиенттік бөлігі жойылған серверге қайта хабарласады да, есеп беруді түрлендіреді. Басым әрекеттердің ұсынылған тізімдерінен тұратын «Толық есеп беру» көбіне қызығушылық тудырады. Қатерді анализ жасау кезеңінде белсенділерді идентификациялау жүргізіледі, олардың сапалы классификациялануы ұсынылады (Бизнеске әсер етуі жоғары, орташа және төмен), сонымен бірге әлсіздіктер мен қауіп-қатер тізімі анықталады. Қатерді бағалау кезінде үш деңгейлі шкала (әсерге шалдыққыштығы жоғары, орташа және төмен) бойынша анықталады. Қауіп-қатердің пайда болу жиілігін бағалау кезінде градациялар қолданылады: жоғарғы (бір жылда бір немесе бірнеше оқиғалардың пайда болу ықтималдығы); орташа (екі-үш жыл аралығында әсер ету пайда болуы мүмкін); төменгі (әсер етудің үш аралығында пайда болуы екіталай).

1.4 Ақпараттық қауіпсіздік қатерін бағалау мен анализдеудің әдістері мен әдістемелері

ҚБАҚ 14 - Байестік желілер негізіндегі әдіс (МБС) [69] операциондық қатерлердің бағалау каузалдық моделін құру үшін өңделген. Оның негізін Байес теоремасы қалап отыр, ал мұндай қатерлерді бағалауда қолданудың құндылығы оның статистикалық және сараптамалық жолмен алынатын оқиғалардың ықтималдығы туралы мәліметтерді қиыстыру қабілеттілігінде болып табылады. Шығындалу статистикасына ие емес қатердің (қауіп-қатер) бөлек факторларына тәуекелді оқиғалар ықтималдығының бағасы тек қана сарапшылық білімдерге негізделген болуы мүмкін, ал басқаларына егер модельдеу мақсатына жеткілікті мәліметтер көлемі жиналған болса, онда-шығындалу статистикасына негізделеді. Әрбір қатермен байланысты болған оқиғаға (мысалы-"Хакерлік шабуыл", "Рұқсат етілмеген қол жеткізу"(РЕҚЖ), "Рұқсат етілмеген модификация" (РЕМ) т.б.) оны жүзеге асыру ықтималдығының және онымен (бір тізбекті) байланысты болған операциялық шығындар бағалауы жүргізіледі. Оқиғаны жүзеге асыру ықтималдығы үздіксіз функция түрінде немесе ықтималдылық кестесі түрінде (дискреттік ықтималдылықтар) көрсетілуі мүмкін. Себебі, үздіксіз функциялардың таралуын тек кейбір жағдайларда ғана ала алғандықтан (статистиканың жеткіліксіздігінен), дискреттік таралулар

қолданылады. Бағанда кіріс көрсеткішіне ие емес драйверлер (факторлар) болып табылатын тұжырымдар үшін әр бір мүмкін болған оқиға шешім абсолютті ықтималдығы көрсетілген болуы қажет, ал өзге тұжырымдар әсер ететін басқалары үшін байланысты болған тұжырымдардың әр бір комбинациясына шартты ықтималдылық көрсетіледі.

Шартты ықтималдылықтың сараптық тапсырмасының үлгісі [69] 1.4 кестеде көрсетілген.

Кесте 1.4 - Ықтималдылықты қалыптастыру

	Шарттың нәтижесі			
Хакерлік шабуыл	ИӘ		ЖОҚ	
Вируспен зақымданғандар	Иә	Жоқ	Иә	Жоқ
Әртүрлі шарттар үшін "Сервердің тоқтауы" оқиға нәтижесінің ықтималдылығы				
Болады	0,3	0,15	0,10	0,02
Болмайды	0,7	0,85	0,90	0,98

Абсолюттік ықтималдылық пен шығын көлемі анықталады. Нәтиженің үш түрі қаралады: қол жетімділіктің (ҚЖ), тұтастықтың (Т), құпиялылықтың (Қ) бұзылуы. Материалды белсенділер үшін шығын шкала бойынша анықталады-белсендіні толық жоғалтудан мүмкін емес уақыт өлшеміне дейін іркілуі (тоқтауы, ақпараттық қауіпсіздікы болуы) [69].

ҚБАҚ 15 - NIST 800-30 [70] (Risk Management Guide for Information Technology Systems, NIST ұсынысы, National Institute of Standards and Technology АҚШ өңдеуші**) әдіснама** тоғыз алғашқы қадамдарды қамтиды: жүйе сипаттамасы; қауіп-қатер идентификациясы (1.5-кесте) [70]; әлсіздіктер идентификациясы (1.6-кесте) [70]; басқару анализі; ықтималдылықты анықтау; әсер ету анализі; қатерді анықтау; басқару бойынша ұсыныстар; нәтижелерді құжаттастыру.

Кесте 1.5 - Қауіп-қатер идентификациясының үлгісі

Қауіп-қатердің қайнар көзі	Себебі	Қауіп-қатер іс-әрекеті
Хакер, крекер	Шақыру Өзімшілдік Бүлік	Хакинг Әлеуметтік инжиниринг Ақпараттық жүйелерге басып кіру, ақпараттық жүйедегі РЕҚЖ-ді бұзу.
Кибер-қылмыскер	Ақпараттың бұзылуы Ақпараттық ашып беру Ақшалай пайда көру Рұқсат етілмеген модификация мәліметтері	Компьютерлік қылмыс (кибер-ізге түсу) Алаяқтық әрекеттер Spoofing ақпараттық сатып алу Ақпараттық жүйеге басып кіру

Қатерді анализдеу процесінде ақпаратты жинақтау, қауіп-қатер идентификациясы (қайнар көзін анықтау, қауіп-қатердің пайда болу себептерімен іс-әрекеттері) жүзеге асырылады. Бағалау үшін мынадай ықтималдылық деңгейлері қолданылады: жоғары «Ж», орташа «О», төмен «Т». Әсеретуді анализдеу кезінде оқиғалар анықталады, ҚЖ, Т мен Қ жоғалтумен байланысты. Әсер ету көлемі шкала бойынша анықталады: жоғары «Ж», орташа «О», төмен «Т». Қатерді анықтау үшін ҚД-нің матрицасы қолданылады: «Ж»; «О»; «Т» [70].

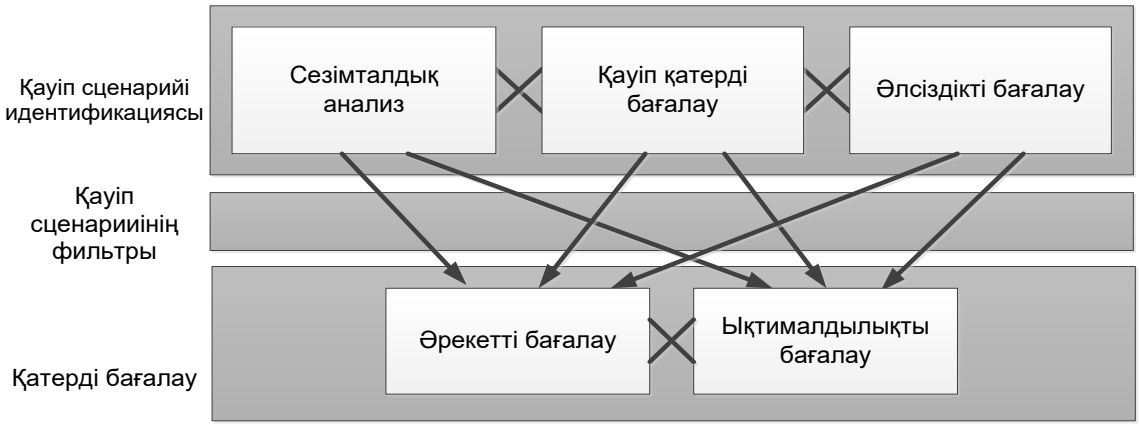
Кесте 1.6 - Әлсіздік пен қауіп-қатер жұбының идентификация үлгісі

Әлсіздік	Қауіп-қатердің қайнар көзі	Қауіп-қатер әрекеті
АЖ жойылмаған жұмыстан босатылған қызметкерлер ID	Жұмыстан босатылған қызметкерлер	Жеке мәліметтер негізінде АЖ-ге ену
Компания Брандмауэрі кіріс telnet байланыстыруларға рұқсат береді және де XYZ серверінде ID қонақ қосылған болады	Рұқсат етілмеген тұтынушылар (мысалы, хакерлер, босатылған қызметкерлер)	telnet қолдану арқылы XYZ серверіне қол жеткізу үшін және ID қонағы бойынша жүйелер файлдарын оқу

ҚБАҚ 16 - VAR (Value at Risk) **әдісі** олардың пайда болу ықтималдығымен (ПБЫ) сәйкестендірілген мүмкін болған жоғалтудың терминдерінде қатерді бағалауға мүмкіндік береді статистикалық тәсілдерге негізделген [68]. Мұнда белгілі бір уақыт кезеңінің аралығында жоғалтудың таралуын болжау квантилі баяндалады. Бағалау процесі мына кезеңдерді қамтиды: қауіп-қатерді идентификациялау, олардың ықтималдылығының бағалары, қатерді төмендету мен қауіптілікті есепке ала отырып құндылылығын шығару. Қауіп-қатер классификациясы бастапқыда жүзеге асырылады, мысалы, алаяқтық, жаман ниетті әрекет, қалжың, жеке ақпаратқа қол жеткізуге талпыну, табиғи апаттар, қаскөйлік, тұтынушылардың қателіктері т.б. Қауіп-қатерлер идентификацияланған кезінде олардың ықтималдылығы (ықтималдылық таралуы) бағаланды, мүмкін болған сценарийлер жазылды, енді қауіп-қатер жүзеге асуы кезінде фирма үшін қауіптіліктер анықталуда. Бағалау процесін инициализациялау үшін сұрақ қолданылады, мысалы, «Бір айлық кезеңде ақпараттық қауіпсіздік ережелері бұзылғандықтан компания қанша белсенділерін жоғалтуы мүмкін?» [68].

ҚБАҚ 17 - TRA әдістемесі (Threat and Risk Assessment, Government (Communications Security Establishment)-Канада өңдеуші компаниясы) [52] IT-жүйесі үшін жетекшіліктің үш түрі негізінде өңделген: қауіпсіздік қатерін

басқару (Guide to Security Risk Management for Information Technology Systems – MG-02); сертификациялар мен акредитациялар (Guide to Certification and Accreditation of Information Technology Systems – MG-01); кепілдікті таңдау мен қатерді бағалау (Guide to risk assessment and safeguard selection for Information Technology Systems MG-03). Қатерді бағалау үшін аналитик алдымен IT-жүйенің сипаттамасын қарастыруы, елеулі қауіп-қатер сценарийін идентификациялауы, ПБЫ-на олардың әсер етуін бағалау керек (сурет. 1.15).



Сурет 1.15 - Қатерді бағалау процесі

Қатерді бағалау процесі кезінде әрбір қауіп-қатердің сценарийі үшін оның әсер етуі мен ықтималдылығы есептеледі. Мұндай тәсіл белгілі бір уақыт кезеңіндегі күтілетін орташа жоғалтуларды бейнелейді [52]. Негізінде мәні жағынан, (R) қатер (V) әлсіздік, (T) қауіп-қатер, (A_{Val}) белсенді құны арасындағы функционалды байланысы: (V): $R = f(A_{Val}, T, V)$ түрінде суреттеледі. Мұндай, корпоративті мәліметтер (КМ) сияқты, белсенділер топ бөлігі үшін қауіп-қатерді (мысалы, «Хакерлік шабуылды») бағалау 1.7-кесте [52] негізінде жүзеге асырылады, мұнда ақпараттық қауіпсіздік сипаттама құпиялылығының (ҚБ), тұтастығының (ТБ) және қол жетімділігінің бұзылуы (ҚЖБ) үш деңгейлі сапалы («Ж», «О»,«Т») шкаласымен беріледі.

Кесте 1.7 - Қауіп-қатерді бағалау үлгісі

Қауіп-қатер класы	Қауіп-қатер әрекеті	Қауіп-қатер агент (ҚА) категориясы	ҚА	Қауіп-қатер оқиғасы	Бұзушылық деңгейі			Белсенділер топ бөлігі
					К	Ц	Д	
Әдейі	Тыңшылық	Хакерлер	-	РҚЖ	Ж	-	-	КМ
	Қасақана	Хакерлер	-	РЕМ	-	-	О	КМ
	Қасақана	Хакерлер	-	DoS	-	Т	-	КМ

ҚБАҚ 18 - FRAP [21] (Facilitated Risk Analysis Process, Peltier and Associates – АҚШ өндеуші компаниясы) **әдістемесі** бес кезеңнен тұратын

қатерді басқару процесі көлемінде қаралатын ақпараттық жүйелердегі ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған. Этап 1 – қорғайтын белсенділерді анықтау (желілерді автоматты анализдейтін (сканерлейтін) құрал-саймандарды қолдану, жүйеге құжаттарды үйрену, сауалнамалар негізінде жүргізіледі). Этап 2 – қауіп-қатерді идентификациялау. Қауіп-қатер тізімін жасаған кезде әр түрлі тәсілдер қолданылуы мүмкін, мысалы: берілген сараптаушылар алдын ала дайындаған тізімдерден ақпараттық жүйе үшін көкейкесті қауіп-қатерді (checklists) таңдау; АЖ-нің мәліметімен байланысты ақпараттық қауіпсіздік оқиғасының статистикасы анализденеді; олардың орташа жылдық жиілігі бағаланады (қауіп-қатермен қатар, мысалы, өрттің пайда болуы, мәліметтерді сәйкесінше мемлекеттік мекемелерден де алуға болады); компания мамандары тапсырманы "миға шабуыл" арқылы шешеді т.б. Этап 3 – Қауіпті бағалау (ҚБ). Құрылған тізімдегі әр бір қауіп-қатерге оның (***ВС₃***) пайда болу ықтималдығын салыстырып қарайды, әрі қарай алынған мәндерге және берілген қауіп-қатердің жасаған (***ВС₆***) шығынын бағалайды, оның деңгейі бағаланады. Қатер анализін жүргізу кезінде жүйенің бастапқы кезеңінде қорғаныс механизмі мен құралдары болмайды. Міне, осылай, қорғалмаған АЖ үшін қатер деңгейі бағаланады, бұл өз кезегінде ақпаратты қорғау (АҚор) құралдарын енгізуден болған салдар екенін көрсетуге мүмкіндік береді. Бір жыл көлемінде келесі шкалаларды қолдану арқылы оның жүзеге асырылуынан болған шығынның және қатердің ПБЫ бойынша бағалау жүргізіледі. Ықтималдылық үшін (Probability): жоғары (High Probability) – ықтимал; орташа (Medium Probability) – мүмкін болған; төмен (Low Probability) –екіталай. Зақымдық арналған - (Impact – белсендіге көрсетіп жатқан шығындалу немесе зиян көрсету көлемінің мөлшері): «Ж» (High Impact) – өте маңызды бизнес-бөлімшелерінің тоқтатылуы имиджді жоғалтуға немесе айтарлықтай пайда ала алмауға, бизнес үшін айтарлықтай зиян алып келеді; «О» (Medium Impact) – қысқа уақытқа өте қиын процесстер немесе жүйелер жұмысының үзілуі бір бизнес-бөлімшеде шектелген қаржылай шығындарға алып келеді; «Т» (Low Impact) – айтарлықтай қаржылай шығындарды тудырмайтын жұмыстағы үзіліс. Бағалау қатер матрицасы қоятын ережелерге сәйкес жүзеге асырылады (1.16-суреттен қара) да, келесі түрде интерпретациялануы мүмкін: *А* деңгейі–қатермен байланысты шаралар (мысалы, АҚ құралдарының енгізілуі) міндетті түрде және дәл сол кезде орындалуы қажет; *В* деңгейі – қатермен байланысты шаралар алдын ала қамдалуы қажет; *С* деңгейінде – жағдайды бақылау қажет болады (бірақ тікелей қауіп-қатерге қарсы әрекеттер бойынша шараларды қабылдаудың қажеті болмауы мүмкін); *D* деңгейі – дәл осы сәтте ешқандай шараларды қолданудың қажеті жоқ [21]. Этап 4 – контршаралардың анықталуы. Қатерді бағалаудан және қауіп-қатерді идентификациялағаннан соң, қатерді жоюға немесе оны қолайлы деңгейге дейін алып баруға мүмкіндік беретін контршаралар анықталады. Этап 5 – Құжаттастыру. Қатерді бағалау мен анализдеуден соң шешімдер стандартталған форматта егжей-тегжейлі құжаттастырылады.

Алынған есеп саясатшыларды, рәсімдерді, Ақпараттық қауіпсіздікіпсіздік бюджетін т.б. анықтау кезінде қолданылуы мүмкін.

IMPACT

PROBABILITY

	High	Medium	Low
High	*A*	*B*	*C*
Medium	*B*	*B*	*C*
Low	*B*	*C*	*D*

A – Corrective action must be implemented
B – Corrective action should be implemented
C – Requires monitor
D – No action required at this time

Сурет 1.16 - FRAP қатерлерінің матрицасы

ҚБАҚ 19 – BSI-Standard100-3 [72] (Risk Analysis based on IT-Grundschutz – IT-Grundschutz негізінде қауіп анализдері, ақпараттық қауіпсіздікіпсіздік бойынша Федеральды Агенттігімен өңделген (Federal Office for Information Security – BSI), Германия) **әдістемесі** BSI-Standard 100-3-де ұсынылған IT-қауіпсіздігінің қатерді бағалау мен анализдеу процесіне негізделеді, жеті кезеңді қамтиды. Кезең 1 – Алдын ала дайындық. Бұл кезеңде ақпараттық қауіпсіздікіпсіздік саласы мен Қ, Т пен ҚЖ-ті қамтамасыздандыру көзқарасы жағынан қаралатын, оған қойылған талаптар (қалыпты, жоғары, өте жоғары) анықталады. Сонымен бірге, ақпараттық қауіпсіздіктің қосымша анализдеу болып табылатын, кәсіпорын құрылымын анализдеу жүргізіледі, оның қазіргі деңгейі бағаланады. Кезең 2 – Қауіп-қатерді сипаттауға дайындық. Әдістемедегі ұсынылған қауіп-қатер тізімінің көмегімен белгілі бір кәсіпорын үшін оларды анализдеу жүзеге асырылады. Кестеге енгізілетін (1.8-кестеде) қорғаныстың арнайы объектілері (АО) мен модульдері идентификацияланады [72].

Кесте 1.8 - Идентификациялау үлгісі

№	Модуль атауы	АО
B 2.4	Солтүстік бөлме	M. Каб 723
B 2.6	Өндірістік бөлме	M. Каб. 811
B 3.101	Сервер	S3
B 3.207	Басты клиент	C4
B 3.301	Шлюз қауіпсіздігі (Firewall)	N3

Ақпараттық қорғаудың әр бір модулі қауіп-қатер тізімімен байланысты, ал оның аты мен номері нақты АО-ге сәйкес келеді. Нақты объектіге қауіп-қатер тізімі кезеңді өтудің шешімі болып табылады (1.9-кестесі) [72].

Кесте 1.9 - Қауіп-қатерді сипаттау үлгісі

Сервер S3
Қ: қалыпты; Т:Жоғары; ҚЖ:өте жоғары
Т1.2 IT-жүйенің істен шығуы Т3.2 Белсендіні абайсызда жою Т4.1 Тамақтанудағы кідіріс Т5.57 Желілік сканерлеу Т5.85 Т ақпаратының жоғалуы т.б.

Әрі қарай жалпыланған кестесінде қауіп-қатер әрбір АО бойынша сұрыпталады. Кезең 3 – Қосымша қауіп-қатерлерді анықтау. Мұнда арнайы сұраныстар жинағы қолданылады, мысалы: «Қандай форс-можорлы әлеуетті жағдайлар ақпараттық салада ерекше қауіп-қатер туғызады?»; «Ақпараттық қауіпсіздікіпсіздікке кепілдік беру үшін ұйымдастырушылықтың қандай кемшіліктерінен қайткен күнде де қашу керек?»; «Адамның қандай қателіктері АҚ-ке теріс әсерін тигізеді?»; «Техникалық бас тартудың себебінен АҚ-тің арнайы қандай проблемалары қаралып жатқан АО-мен болуы мүмкін?» т.б. Кезең 4 – Қауіп-қатерді бағалау. Мұнда қор сұраныстары негізінде мамандардан тақырыптық сауалнама жүргізіледі. Әрбір бөлек қауіп-қатер үшін Y (егер ақпараттық қауіпсіздік шаралары (жүзеге асырылған немесе көзделген), бірқатар қауіп-қатерден тиісті қорғауды қамтамасыз еткенде немесе қатер дәрежесінің ағымдағы анализі үшін қауіп-қатер маңызды емес болғанда) немесе N көрсеткішімен (егер ақпараттық қауіпсіздік шаралары (жүзеге асырылған немесе көзделген), бірқатар қауіп-қатерден тиісті қорғауды қамтамасыз етпегенде) нәтижелері кестеде белгіленіп отырады (1.10-кесте) [72].

Кесте 1.10 - Қауіп-қатерді бағалау үлгісі

Сервер S3	ҚҚБ
Қ: қалыпты; Т: жоғары; ҚЖ: жоғары	
Т 1.2 IT жүйесінің істен шығуы	N
АҚ шаралары S3 сервері үшін қауіп-қатердің жүзеге асуын жоққа шығармайды. IT – шаралары Grundschutz Каталогы бойынша сәйкес келмейді	
Т 5.85 Ақпараттың Т жойылуы	N
Клиенттің тапсырыс жөніндегі ақпаратты PEM ұшырамауы тиіс. Болмаса бұл жеткізілімнің артылуына (жетіспеуіне) алып келуі	

мүмкін, сонымен бірге компанияны көптеген шығынға ұшыратуы мүмкін.	

Кезең 5 – Қатерді өңдеу. Мұнда шкала қолданылады: «*A*» – қосымша шаралар көмегімен қатерді төмендету; «*B*» – құрылымын өзгерту арқылы қатерді тоқтату; «*C*» – қатерді қабылдау; «*D*» – қатерді жіберу; (1.11-кесте) [72]. Кезең 6 – АҚ тұжырымдамасының шоғырлануы. Кезең 7 – Кері байланыс [72].

Кесте 1.11 - Қатерді өңдеу кестесінің үлгісі

Сервер S3	
Қ: қалыпты; Т: жоғары; ҚЖ: жоғары	
Т 1.2	IT жүйесінің істен шығуы
«*A*» S 6. U1	АҚ бойынша қосымша IT-шара: Клиентпен сөйлесу үшін жүйені толық ауыстыруды жүзеге асыру. Клиентпен байланысу үшін жүйені толық ауыстыруды жүзеге асыру. Байланыс каналдарын қоса бұл барлық техникалық құралдарға тиісті. Е.3. бөлмесінде резервтік жүйе орналасқан. Кез келген уақытта қолану мүмкіндігімен, (емес > 30 мин. Өндіріс іркуі). Клиентпен модемді байланыс қолданылады. Жүйенің барлығының ауысуы, модемді байланыстыруды қоса, үш айда бір рет тексеріледі, сонымен бірге әрқашан конфигурацияның өзгеруі кезінде тексеріледі.
Т 5.85	Ақпараттың Т-ң жоғалуы
«*C*»	Қатерді қабылдау: Қатер өткізу жүйесі мен IT-жүйесіне енгізіліп құрылған АҚ-ң механизмдерімен белгілі бір дәрежеге дейін минимумдалғанмен әрі қарай оқиға өрбуі мүмкін, бұл өз кезегінде тапсырысты талап ету туралы ақпараттың РЕМ алып келетіндіктен бұл компанияны үлкен қатерге ұшыратады. Бұл қалдық қатер басшылықпен қабылданған, себебі тиімді қарсы әрекеттер экономсыз болмақ.

ҚБАҚ 20 - РС БР ИББС-2.2-2009 [64] (Ресей банк стандарттау саласындағы ұсыныстар, банктік жүйесіндегі ұйымдардың ақпараттық қауіпсіздігін қамтамасыз, Ресей Федерациясы) **әдістемесі** алдын ала белгіленген саласына кіретін ақпараттық белсенділер (АБ) типі үшін АҚ-тің бұзылу қатерін бағалау мен анализдеуді бағалаудың жүргізіледі. Бастапқы кезеңде анықталатын: бағалар саласына кіруші (оларды топтастыру шешімдерінің негізінде) АБ типтерінің толық тізімі; бағалау саласының әрбір АБ типтеріне сәйкес келетін орта объектілерінің типтерінің толық тізімі; ақпараттық инфрақұрылым иерархиясының барлық деңгейіндегі бөлінген барлық орта объектілерінің типтеріне негізделген ақпараттық қауіпсіздік қауіп-қатерінің моделі анықталады. АБ бұзылу қатерін бағалау қауіп-қатерді жүзеге

асыру ықтималдылық С бағалау (АБ қауіп-қатерін жүзеге асыру мүмкіндігінің дәрежесі-түп нұсқасында ЖАМД) мен оның (қарастырылып жатқан АБ типтері үшін АҚ қасиетін жоғалтудан кейінгі салдардың ауырлық дәрежесі түп нұсқасында-САД) жүзеге асуының потенциалды зияны негізінде анықталады.

Баға IT саласы кәсіпқойларын қатыстыру арқылы АҚ қызмет мамандарының сараптық пікіріне негізделіп анықталады. Қосымша, қарастырылып жатқан АБ типтерін қолданушы бейінді бөлімше қызметкерлерін қатыстыру қажет. АҚ-тің бұзылу қатерін бағалауды жүргізу үшін 6 рәсім орындалады: АБ типтер тізімін анықтау, ол үшін бағалау орындалды (яғни қатерді бағалау саласы). Компания толығымен қаралуы мүмкін, оның бөлек бөлігі немесе бөлек процессі қаралуы мүмкін. Әрбір АБ типі үшін қандай АҚ (Қ, Т, ҚЖ және қажет кезінде басқа) құралдары қамтамасыздандырылуы қажет екенін анықтау; 2. АБ типтерінің әр біріне сәйкес келетін орта объектілерінің типтер тізімін анықтау (ақпараттық инфрақұрылым деңгейі бойынша бөледі); 3. Көкейкесті қауіп-қатер (компанияның қауіп-қатер моделінің негізінде қалыптасады) қайнар көздерінің тізімін көрсетілген әрбір типтер үшін анықтау; 4. Орта объектісінің типтеріне қатысты қауіп-қатердің ЖАМД анықтау. Қауіп-қатер әсерінің нәтижесінде әрбір АБ типі үшін бес сатылық С шкаласының («жүзеге асырылмайтын» (ЖА), «минимумды» (МН), «орташа» (ОР), «жоғарғы» (ЖО), «критикалық» (КР) негізінде АҚ қасиетінің жоғалу мүмкіндігінің анализі жүргізіледі. АҚ қауіп-қатерін ЖАМД бағалау үшін негізгі факторлар болып табылатын: сәйкес келетін қауіп-қатер модельдерінің ақпараты (қауіп-қатердің орналасқан жері мен оның уәждемесі туралы мәліметтер және қайнар көзінің (ресурстар) сарапануы туралы болжамдар), қауіп-қатерді өткен шақтағы оның қайнар көзімен жүзеге асыру жиілігі туралы мәліметтердің статистикасы, қауіп-қатерді жүзеге асыру жолдары мен оларды анықтаудың қиынға соғуы туралы ақпарат, сонымен бірге қарастырылып жатқан орта объектілерінің типтерінде ұйымдастырушылық, техникалық және т.б. априорлық қорғау шараларының бар болуы туралы мәліметтер; 5. Қауіп-қатер қайнар көзі шығарған оларға сәйкес келетін орта объектілерінің типтеріне әсері нәтижесінде АБ типтерінің әрбірі үшін АҚ әрбір маңызды қасиетін жоғалту салдарының анализі негізінде АҚ типтері үшін САД анықтау. Төрт сатылы («МН», «ОР», «ЖО», «КР») С шкаласы қолданылады. Бағалаудың негізгі факторлары: компания қызметінің беделі мен үздіксіздігіне әсер ету дәрежесі болып табылады; АБ АҚ қасиетін қайта қалыптастыруға қаражаттық (материалды) жоғалтулар мен шығындар көлемі (АҚ бұзылуының салдарын-қаражаттық, материалдық, уақытша және адамдық ресурстарын жою); заң талаптарының (компанияның келісім-шарт міндеттемесінің) бұзылуының дәрежесі, сонымен бірге АҚ саласындағы бақылаушы және реттеуші ұйымдардың талаптары; қарастырылып жатқан орта объектісінің типіне сәйкес келетін сақталатын, қолдан қолға өткізілетін, өңделетін және жойылатын ақпараттар көлемі; қарастырылып жатқан орта объектісінің типінде салдардың (апостериорлы) ауырлығын төмендететін ұйымдастырушылық, техникалық және тағы басқа қорғау шараларының бар

болуы туралы мәліметтер; 6. АҚ бұзылу қатерін бағалау қауіп-қатерді ЖАМД мен сәйкес келетін қауіп-қатердің жүзеге асуының себебінен АҚ бұзылуының САД негізінде жүргізіледі. Бағалау бар болған барлық оларға сай келетін орта объектілерінің типтерінің қисындастыруларына және оларға әсер етуші қауіп-қатердің қайнар көздеріне, АБ типтерінен бөлініп шыққан АҚ-тің барлық мәнді қасиетіне жүргізіледі. Қатердің келесі С шкаласы қолданылады: мүмкін (М), мүмкін емес (МЕ). Қауіп-қатердің ЖАМД мен САД-н салыстыру үшін АҚ-ң бұзылу қатерлерінің мүмкін және мүмкін емес кестесі толтырылады (1.12-кесте) [64].

Кесте 1.12 – Мүмкін (М) және Мүмкін Емес (МЕ) қатерлері

Ақпараттық қауіпсіздік қауіп-қатерінің ЖАМД	Ақпараттық қауіпсіздік бұзылуының САД			
	МН	ОР	ЖО	КР
МН	М	М	М	Д
ОР	М	М	М	МЕ
ЖО	М	М	МЕ	МЕ
КР	М	МЕ	МЕ	МЕ
МН	МЕ	МЕ	МЕ	МЕ

АҚ қауіп-қатерінің ЖАМД бағаларының (мысалы, % -да) және компания капиталының көлемінен (ККК) (мысалы, ақшалай түрде) САД негізінде АҚ бұзылу қатері С (ақшалай) түрінде бағалануы мүмкін. Санды бағалау да экспертті әдістермен жүзеге асырылады. Қажет кезде, САД пен қауіп-қатердің ЖАМД С мен С бағаларының сәйкес келу шкалалары (1.13-суреті) [64] қолданылуы мүмкін.

Кесте 1.13 - Сәйкес келу шкалалары

Қауіп-қатердің ЖАМД		Ақпараттық қауіпсіздік бұзылу САД	
($М_{кч}$)	($М_{кл}$), %	($М_{кч}$)	($М_{кл}$), %
МН	0	МН	[0; 0,5[
ОР	]0; 20[	СР	[0,5; 1,5[
ЖО	[20; 50[	ВС	[1,5; 3,0[
КР	[50; 100[	КР	[3,0; 100] (ККК-дан)
МН	100		

АҚ-тің бұзылу қатерінің сандық бағалау қауіп-қатердің ЖАМД мен САД бағалар АБ типтерінен бөлініп шыққан АҚ-тің маңызды қасиеттерінің әр біріне, әр бір оларға сай келетін барлық орта объектілерінің типтерінің қисындастыруларына және оларға әсер етуші қауіп-қатердің қайнар көздеріне туынды болып табылады, жасау болып табылады. Компанияның жалпы қатерді бағалауы АҚ-тің бұзылу қатері бойынша бағалау Санды сумма ретінде

есептеледі. Сонымен бірге, әдістемеде ұсынылған класстардың тізімі мен АҚ қауіп-қатерінің қайнар көзінің тізімі бар [64].

1.5 Ақпараттық қауіпсіздік қатерін бағалау мен анализдеуде басқада тәсілдер

ҚБАҚ 21 - ISO/IEC 27005:2008 [4, 5] (Information technology – Security techniques – Information security risk management (Ақпараттық технология – қорғаныс әдістері – АҚ қатерінің менеджменті) стандарттарды техникалық тұрғыдан ISO/IEC TR 13335-3:1998 және ISO/IEC TR 13335-4:2000 болдырмау мен ауыстыру, қайта қарауды ұсынады, Швейцария) **стандарты** Ақпараттық қауіпсіздік қатері бар менеджментке, көбінесе ISO/IEC 27001 сәйкес «Ақпараттық қауіпсіздік менеджмент жүйесі» (ISMS) талабын қолдай отырып ұсыныстар береді. Менеджмент процесі алты кезеңде жүзеге асырылады.

1-кезең – Мәнмәтін жасау. Мәнмәтінді жасауға қатысты ұйым туралы барлық мәліметтердің жалпы анализі жүзеге асырылады, сонымен бірге ақпараттық қауіпсіздік қатерлер менеджменті үшін қажет негізгі критериилерді орнату және ол үшін қолдану аясы мен жүзеге асыру шекарасын анықтау жүргізіледі.

2-кезең – Қатерлерді бағалау. Бұл жерде ұйымға қатысты (белсенділер, қауіп-қатерлер, бар болған талаптардың, әлсіздіктер мен салдар) индентификация, (сан, сапалық немесе олардың қисындасуын) бағалау мен сипаттау, қатерлердің басымдылығына қарай орналастыру жүзеге асырылады. Сапалы баға потенциалды салдар көлемін (мысалы, төмен, орташа немесе жоғары) және ықтималдылығын, осы салдар болатынын, сипаттау үшін атрибуттардың біліктігін қолданады. Сандық бағалау сандық мәндердің көлемін салдарға сияқты, ықтималдылықтарға да қолданады. Сандық бағалау көп жағдайда қақтығыстар статистикасын қолданады. Салдар бағасы берілген кезеңді өтудің нәтижелері, қақтығыс ықтималдығы мен ҚД болады.

3-кезең – Қатерлерді өңдеу. Жалпы өңдеу, сонымен бірге төмендеу, сақтау, болдырмау және қатерді өткізу сипаттамасын өз ішіне алады.

4-кезең – Қатерді қабылдау. Қатерді өңдеу жоспары қабылдаушы критерийге дейін бағаланған қатерлер қалай өңделгенін сипаттауы қажет.

5-кезең – Қатер байланыстары. Қатерлерді басқару бойынша келісімге жету мақсатында шешім қабылдаушы тұлғалар мен өзге қатысы бар жақтардың арасындағы қатерлер туралы ақпарат алмасу.

6-кезең – АҚ қатерін қайта қарау мен мониторинг. Мұнда қатер факторларын қайта қарау мен мониторинг, сонымен бірге оның менеджментінің жақсартылуы жүзеге асырылады. Стандартта: қатерді төмендету бойынша шектеулер (F үстемесі); қатерді бағалауға амалдар (E үстемесі, 3 – 18-кестелері [4, 5]); әлсіздіктер мен оларды бағалау әдістеріне (D үстемесі, 1.15-кестесіндегі аппараттық құралдар үшін әлсіздіктерді қара [4, 5]); әдеттегі қауіп-қатерлер (C үстемесі, 1.14-кестесі [4, 5], мұндағы белгілер келесі мәндерге ие: D – біле тұра (ақпараттық қауіпсіздік бағыттарған, алдын ала мақсатталған акциялар), A – кездейсоқ (АБ-де адамның аңдаусызда істеген

әрекеті) және Е – экологиялық (адам әрекетіне негізделмен қақтығыстар); әсер ету құны, белсендінің құндылығы мен идентификациясы (В үстемесі); қатерлер менеджмент процесінің шегінің аясы мен қолдану аясын анықтаудың (А үстемесі); ұсыныстары мен мысалдары бар. ПА-да жүзеге асыруға ие, мысалы, Meycor KP (Knowledge Provider).

Кесте 1.14 - Әдеттегі қауіп-қатер үлгісі

Типі	Қауіп-қатер	белгілер
РЕМ	Рұқсат етілмеген құрал-жабдықтарды қолдану	D
	ПҚ алаяқтықпен көшіру	D
	Жасанды немесе көшірілген ПҚ-ды қолдану	A, D
	Мәліметтердің бұрмалануы	D
	Мәліметтерді заңсыз өңдеу	D

ISO/IEC 27005:2008-де ақпараттық қауіпсіздік қатерін детальді және жоғары деңгейлі бағалау ұсынылған. Соңғысы үшін алдын ала анықталған мәнді матрица қолданылуы мүмкін (1.15-кестесін қарау [4, 5]). Әрбір белсенді үшін бар болған келесі әлсіздіктер мен қауіп-қатерлер қарастырылады, мысалы, егер белсендінің құндылығын – БҚ=3, қауіп-қатердің пайда болу ықтималдығы – ҚҚПБЫ=«В» және әлсіздіктің қарапайым қолданылуы – ӘҚҚ=«Н» онда қатер шаралары – ҚӨ=5.

Кесте 1.15 – Мысалдар

Әлсіздіктер	Қауіп-қатерлер
Жеткіліксіз қызмет көрсету (дефекттік инсталляция)	АЖ-ні жөндеу мүмкіндігіне аласын
Мерзімді ауыстыру үшін ақпараттық қауіпсіздік кестесі	Құрал-жабдықтың бұзылуы (тасмалдаушы)
Кескіндеме өзгеруін енгізуді тиімді бақылау ақпараттық қауіпсіздіклары	Қолданудағы қателік
Қуат берудің төмендеуіне төзімділігі	Қуат беру көздерінің жоғалуы
Қорғансыз сақтау	Тасымалдаушы ұрлығы (құжаттарды)
Жою кезіндегі сақтықтың жеткіліксіздігі	Тасымалдаушы ұрлығы (құжаттарды)
Бақылаусыз көшіру	Тасымалдаушы ұрлығы (құжаттарды)

Сонымен бірге, қақтығыс сценариінің ықтималдылығын (ҚСЫ) анықтау матрицасы ұсынылған еді (1.17-кестесін қара [4, 5], мұндағы «ӨТ» (өте төмен), «Т» (төмен), «О» (орташа), «Ж» (жоғары), «ӨЖ» (өте жоғары), сәйкесінше (тым екіталай), (екіталай), (мүмкін), (ықтимал), (жиі) білдіреді. Нәтижесінде алынатын қатер мәні 0-ден 8-ге дейінгі шкаламен өлшенеді (мысалы, «Т» (0-2);

«О» (3-5); «Ж» (6-8), қатерді қабылдау критерияларына қатысты бағалануы мүмкін.

Кесте 1.16 - ҚӨ бағалау матрицасы

ҚҚПБЫ		Т			О			Ж		
ӘҚҚ		Т	О	Ж	Т	О	Ж	Т	О	Ж
БТ	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	**5**	6	7
	4	4	5	6	5	6	7	6	7	8

Стандарт үстемесінде қатер шаралары арқылы қауіп-қатерлерді саралау үлгісі қаралған (1.17-кестесін қара [4, 5]).

Кесте 1.17 – Қақтығыс сценариінің ықтималдылығын анықтау матрицасы

	ҚСЫ	ӨТ	Т	О	Ж	ӨЖ
Бизнеске әсер етуі	ӨТ	0	1	2	3	4
	Т	1	2	3	4	5
	О	2	3	4	5	**6**
	Ж	3	4	5	**6**	**7**
	ӨЖ	4	5	**6**	**7**	**8**

Матрица (әлсіздіктің аспектілерін есепке ала отырып) ҚҚПБЫ-мен (БҚ) салдар факторларын байланыстыру үшін қолданылуы мүмкін. Алдын ала белгілі бір шкала бойынша (мысалы, 1 ÷ 5) қауіп-қатерде жатқан әрбір белсендіге (b) бағаны) БҚ бағалауы жүргізіледі. Әрі қарай, мысалы, осы шкала бойынша әрбір қауіп-қатер үшін ((c) бағаны) ҚҚПБЫ бағаланады да, алынған нәтижелер бойынша d=b×c көбейту жолы арқылы қауіп өлшемі ((c) бағаны) есептеледі. Салдарынан қатер өлшеміне сәйкес тәртіпте (1.18-кестесінде [4, 5] 1 – ең төмен ҚҚПБЫ мен ең төмен салдар. (a) бағанында қауіп-қатер индентификаторы суреттелген) қауіп-қатерді ((e) бағалау) саралау жүргізіледі.

Кесте 1.18 - Қауіп-қатерді саралау үлгісі

(a)	(b)	(c)	(d)	(e)
A	5	2	10	2
B	2	4	8	3
C	3	5	15	1
D	1	3	3	5

1	2	3	4	5
E	4	1	4	4
F	2	4	8	3

Қатер ықтималдығы және олардың мүмкін болған салдары үшін мәндерді бағалаудың (стандартта берілген) үлгісін қарастырайық. Мұнда көбіне ақпараттық қауіпсіздік қақтығысының салдарына (қақтығыстардың сценариіне) және қандай жүйелерге ерекше назар аудару керектігін анықтауға көңіл бөлінеді. Бұл әрбір қауіп-қатер мен белсенді үшін екі мәнді бағалау жолымен орындалады, бұлардың амалдары балдарды ($Б_{ij}$) белгілейді, мұндағы *i* және *j* – сәйкесінше белсенді мен қауіп-қатер номері. Белсенділердің барлық балдарының қосындысы ҚӨ анықтауға мүмкіндік береді. Бастапқыда әрбір белсендіге сәйкес келетін қауіп-қатердің пайда болу жағдайына БҚ беріледі. Бұл мән қауіп-қатерді жүзеге асыру кезінде пайда болуы мүмкін болған жағымсыз салдармен байланысты. Әрі қарай қатер ықтималдығының көрсеткіші (ҚЫК) анықталады. Ол ҚҚПБЫ мен ӘҚҚ амалдарыннан шыға бағаланады (1.19-кестесін қарау [4, 5]). Сонан соң ҚЫК мен БҚ мәндері 1.15-кестесі [4, 5] сызықты кесіп өтуіне байланысты бар болған балдар беріледі.

Осыдан кейін, әрбір белсенді бойынша қорытынды мән алу үшін олар есептеледі.

Кесте 1.19 - Бағалау үлгісі

ҚҚПБЫ	Т			О			Ж		
ӘҚҚ	Т	О	Ж	Т	О	Ж	Т	О	Ж
ҚЫК	0	**1**	2	1	2	**3**	2	3	4

Келесі мысалдарда барлық мәндер кездейсоқ түрде таңдалған. Айталық О жүйесі үш белсендіге $Б_1$, $Б_2$, $Б_3$ ие және осы жүйеде екі $ҚҚ_1$, $ҚҚ_2$ қауіп-қатер бар дейік. $БҚ_1$=3, $БҚ_2$=2 және $БҚ_3$=4 болсын. Егер $А_1$ мен $У_1$ үшін $ҚҚПБЫ_{11}$=«Т» және $ӘҚҚ_{11}$=«О» болса, онда $ҚЫК_{11}$=1 мәні (1.19-кестесін қара [4, 5]) болады. $Б_1$ мен $ҚҚ_1$ үшін балдар $БҚ_1$=3 және $ҚЫК_{11}$=1 қиылысқан сызығында, яғни $Балл_{11}$=4 болған 1.20-кестесінен [4, 5] шығарып тасталуы мүмкін. Осыған ұқсас түрде, $Б_1$ мен $ҚҚ_2$ үшін $ҚҚПБЫ_{12}$=«О» болсын, ал $ӘҚК_{12}$=«Ж» болсын, онда $ҚЫК_{12}$=3 болады, яғни $Қау_{12}$=6 болады. Енді $КорытБалл_1$=$Қорыт_{11}$+$Қоыт_{12}$=10 барлық қауіп-қатерге байланысты (әрбір белсенді мен оның қауіп-қатеріне) белсендінің қорытынды балдары (Қорыт $Балл_i$) есептелуі мүмкін. Барлық жүйе бойынша қорытынды балды есептеу (ЖҚорытБал) әрбір белсенінің сәйкесінше әрбір қауіп-қатердің барлық балдарының қосынды жолымен жүзеге асырылады ЖҚорытБал =$КорытБал_1$+$КорытБал_2$+$КорытБал_3$ [4, 5]. ISO/IEC 27001 мен 27002 стандарттарында АБ қатерін бағалау кезеңінде ISO/IEC TR 13335-3 құжатына сілтеме беріледі, бұл қазір ISO/IEC 27005 түрінде берілген.

Кесте 1.20 - Баллдық

ҚЫК	АБ				
1	2				
0	0	1	2	3	4
1	1	2	3	**4**	5
2	2	3	4	5	6
3	3	4	5	**6**	7
4	4	5	6	7	8

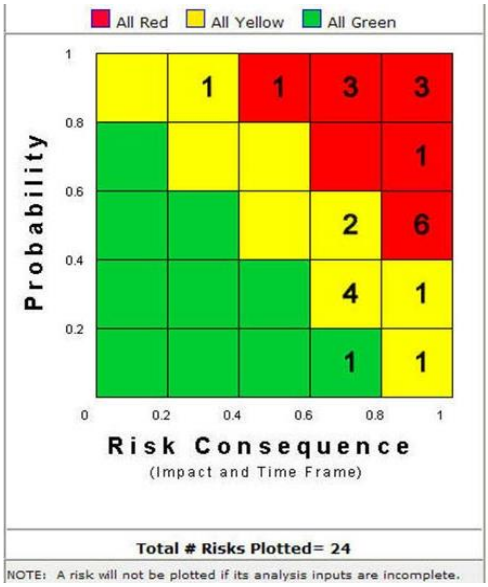
САОР 22 - Risk Matrix [73] (Mitre Corporation АҚШ өндеуші компаниясы) **әдістемесі** қатерді бағалауға бағытталып, нәтижесінде Microsoft Excel үшін үстеме түрінде өңделген еді. Процестің негізне: қатер дәрежесін бағалауды жобалау; тапсырмалардың немесе талаптардың идентификациясы; анықтаулар; сараптау; қатер рейтингін құру; әрекеттер жоспарын басқару; қатерді бағалаудың үздіксіздігі кіреді.

Басынан бастап «Миға шабуылды» сарапшылардың қолдану көмегімен қатер идентификациясы жүргізіледі. Әрі қарай әрбір қатерге, мысалы, уақыт аралығы (мүмкін болған жүзеге асырудың басталу күні мен аяқталуы) мен ПБЫ сияқты әр түрлі ерекшеліктер беріледі. «Егер қатер …, онда оның салдары …» сценарии көмегімен қатер матрицасы құрылады. Әсер етуді анықтау үшін: С (өте қиын); S (маңызды); M_o (орташа); M_i (төмен); N (маңызды емес), ал ықтималдылықтар үшін – (***BC₃***): 0-10% (өте төмен); 11-40% (төмен); 41-60% (орташа); 61-90% (орташадан жоғары); 91-100% (жоғарғы) шкаласы қолданылады.

Кесте 1.22 - Қатер шкаласы

ҚЫК (%)	Әсер ету категориялары				
	N	M_i	M_o	S	С
0-10	Т	Т	Т	О	О
11-40	Т	Т	О	О	Ж
41-60	Т	О	О	О	Ж
61-90	О	О	О	О	Ж
91-100	О	Ж	Ж	Ж	Ж

Сараптау кезеңінде Borda әдісі қолданылады да, әрі қарай қатер рейтингі оның дәрежесінің – «Т», «О» немесе «Ж» 1.22-кестесінде анықталуымен құрылады [73]. Артығырақ қатерді анықтау үшін жиілік диаграммасы қолданылады (1.17-суретті қара). Қатер матрицасына мысал 1.18-суретінде берілген [73].



All 5x5 Cells: Red

Risk ID	Risk Name	Consequence	Probability	Mitigation
INF.003	Platform System Integration	0.91	1.00	Yellow
MGT.001	Organizational Interfaces	0.89	0.90	White
OPS.003	Ground Sampling Collection and Analysis	0.84	1.00	Green
SE.016	Technology Readiness for Science Payload CIs	0.87	0.70	Red
SE.015	Cannot handle real-time transmission rate	0.91	0.60	Red
PROG.001	Stakeholder and Mission Partner Complexity	0.73	0.90	Red
SE.017	Balloon weight	0.89	0.50	White
OPS.006	Balloon inflation	0.82	0.60	Yellow
MGT.002	WBS	0.81	0.60	White
OPS.009	Accurately controlling vehicle altitude in the Venusian environment	0.84	0.50	White
SE.005	Component single point of failure	0.81	0.50	Green
APPS.001	SW Testing Enviroment	0.67	1.00	Yellow

Сурет 1.17 - Жиілік диаграммасы

	A	B	F	G	H	J	K	O	P	U
1	Risk No.	Related Risk	RISK	Timeframe Start	Timeframe End	I	Po (%)	Borda Rank	R	Manage/Mitigate
2	1	4	IF contract is not awarded before 30 Sep, THEN program loses $8M in expiring funds.	30 Jan 1999	30 Sep 1999	C	60%	0	H	Use existing Task Order contract to assure award before 30 Sep.
3	2	N/A	IF unmodified commercial laptops are used, THEN operational availability cannot be met in intended environment.	28 Feb 1999	28 Feb 2000	S	100%	0	H	Limit buy for first release and plan technology insertion for improved environmental performance for second release.
4	3	4	IF DII COE V1.5 is more than 1 mo. late, THEN first release will slip day for day.	30 Jan 1999	30 Oct 1999	S	90%	3	M	Use DII COE V1.4 for first release and modify requirements.
5	4	1,3	IF first release is not demonstrated in EFX, THEN program will be assigned to Navy.	15 Feb 1999	15 Apr 2000	C	60%	0	H	Integrate only those capabilities available at contract award for first release.
6	5	1	IF all KPPs must be satisfied by second release, THEN program funding is insufficient.	30 Jan 1999	30 Jul 2001	S	40%	4	M	Use CAIV to prioritize release content subject to budget and plan for third and fourth release.

RiskEntries / ChartI / ChartPo

Сурет 1.18 - Қатер матрицасының үлгісі

ҚБАҚ 23 - AS/NZS 4360:2004 [65] (қатер-менеджмент стандарты, Австралия мен Жаңа Зеландия) **стандарты** жеті кезеңде өтетін қатерді бағалау мен анализдеу бойынша ұсыныстарды береді.

1. Қатер дәрежесін бағалау мән мәтінін анықтау. Қатер-менеджменті мен қатерді бағалау критерий мәнмәтіні орнатылады және анализдеу сұлбасы анықталады.

2. Қатер идентификациясы инициализацияға негізделеді 1.23-кестесі [65].

3. Қатер дәрежесінің анализі. Басқару құралдарының бар болған бағалауы мен идентификациясы жүргізіледі. ҚД мен ықтималдылық салдары қатер матрицасының көмегімен анықталады (1.24-кестесі [65]).

4. Қатер бағасы. Алдын ала орнатылған критериялар мен бағаланған ҚД салыстырылады да, жағымсыз салдар мен потенциалды пайда арасындағы теңгерім қаралады.

5. Қатерді өңдеу.

6. Бақылау.

7. Кеңестер [65].

Кесте 1.23 - Қатерді анализдеу мен идентификациялау

Қатер сілтемесі	Қатер Не болуы мүмкін?	Қайнар көзі Бұл қалай болуы мүмкін?	Қатердің жүзеге асуынан әсер ету	Басқарудың ағымдағы стратегиялары мен олардың тиімділігі (А) – адекваттық; (М) – бірқалыпты; (І) – жеткіліксіз.	ҚД			Тиімділігі
					Ықтималдылық	Салдары	Ағындағы ҚД	

Кесте 1.24 - Қатер матрицасының үлгісі

Мұндағы, Е – Төтенше қатер (талап етілетін әрекет жоспарын детальдау қажет); Н –Жоғарғы қатер (жоғары басқарушының көңіл бөлуі қажет); М – Орташа қатер (басқарушылық жауапкершілікті анықтайды); L – Төмен қатер (әдеттегі рәсімді өңдеу).			Бизнес-процесс& Жүйелер	Салдар				
				Егер толық кестеге әсер етпей шамалы кідірісті талап ететін немесе түзету әрекетін талап ететін жүйедегі немесе процестегі болар-болмас қателіктер болса,	Егер әр кез кездесе бермейтін процесуалдық-стратегиялық норма немесе қажеттілікті толық қанағаттандыра алмайтын қызмет көсету болса,	Егер бір немесе онан да көп шешуші талаптар орындалмаған жағдайда,	Үкімет күн тәртібімен стратегия ның сәйкессіздігі. Даму бағыты қызмет көрсетудің төмендеп бара жатқанын көрсетіп тұр.	Өте қиын жағдайда жүйенің істен шығуы, стратегиялық жоспардың төмендігі немесе бақылаусыздықт ың жалғасуы. Бизнес өте қатты зиян шекті.
			Қаражаттық	Бюджеттің 1%-нан немесе <$5мың.	Бюджеттің 2.5%-нан немесе <$50мың.	>Бюджеттің 5% нан немесе <$500мың	>Бюджеттің 10% нан немесе <$5мил.	>Бюджеттің 25% нан немесе> $5мил.
				Айтарлықтай емес	Кішкентай	Бірқалыпты	Үлкен	Апаттық
Ықтималдылық	Ықтима лдылық	Статис-тика			1	2	3	4	5
	10 кезінде > 1	Көп жағдайда болады	5	Ешбір дауссыз	М	Н	Н	Е	Е
	10 - 100 кезінде 1	Мүмкін, болар	4	Ықтимал	М	М	Н	Н	Е

2	3	4	5	6	7	8	9	10
100 – 1000 кезінде 1	Болашақта болуы мүмкін	3	Мүмкін	L	M	M	H	E
1000 – 10000 кезінде 1	Болуы мүмкін, бірақ күмәнді	2	екіталай	L	M	M	H	H
10000 – 100000 кезінде 1	Төтенше жағдайда болуы мүмкін	1	сирек	L	L	M	M	H

ҚБАҚ 24- Mehari [74] (Clusif-өңдеуші, Франция) **әдіснамасы** Clarion жүйесін ауыстырады да, қатерді бағалауға құрылымдық өту болып табылады. Ол Сап мен Сан-ға ҚД мен қатер факторын бағалауға мүмкіндік береді. Солай бола тұра, Mehari ISO/IEC 27005:2008 берілген минималды әдістерге маңызды толықтырушы болып табылатын құралдарды (мысалы, формулаларға, бағаларға т.б. қойылған талаптарды) және білім қорларын (сондай-ақ ақпараттық қауіпсіздік диагностикасына арналған шаралар) біріктіреді. «Қандай қатер ұйымдастыру үшін жоғары болып табылады және олар қолайлы немесе жоқ болып табылады?» сұрағына жауап беру үшін, қатердің мүмкін болған барлық оқиғасын шығару үшін, олардың ішінен маңыздырағын жеке тұлға ретінде анықтау үшін, сосын қатерді ыңғайлы деңгейге дейін төмендету бойынша әрекетті айқындау үшін құрылымдасқан амал. Бағалау үшін негізгі екі нұсқа ұсынылады – (Microsoft Excel, Open Office-те интеграцияланатын) білім қорын қолдану немесе ПҚұр қолдану (мысалы, толығырақ тұтынушы интерфейсін қамтамасыз ететін және алынған нәтижелерді оңтайластыруға, көрнекіліктеуге, модельдеуге мүмкіндік беретін Risicare). Бағалау үшін «қатердің төмендеу факторын» есепке алатын қатердің құрылымдасқан моделі қолданылады [74]. Қатерді бағалау процесі 9 кезеңде жүзеге асырылады: **1**. Қатер идентификациясы. Екі амал ұсынылады – тура (ақпараттық қауіпсіздік бұзылуына алып келуі мүмкін оқиғаның немесе жарамсыздықтың идентификациясын қарастырады, нәтижесінде мүмкін болған жарамсыздықтар типі сипатталады) және жүйелілік (автоматтандырылған бағаларды енгізу үшін кең көлемді білім қорын қолдануда өз шешімін табады). **2**. Әсер ету бағасы. Мұнда Сап шкала қолданылады, бұл жерде: 1 – өте төмен экспозиция (ақпараттық қауіпсіздік кез келген шараларына қарамай, мұндай сценарий - өте төмен болып өту ықтималдығы); 2 – әсер етуі төмен (мұнда сценарий қысқа мерзімді немесе орта мерзімді уақытта болып өту ықтималдығы – төмен); 3 – орташа экспозиция (егер ештеңе жасамасақ, онда мұндай сценарий қысқарақ мерзімде болып өтуі қажет); 4 – жоғары деңгейде әсер ету (егер еш бір нәрсе жасалмаса, онда мұндай сценарий қысқа мерзімде құтылу мүмкін емес). **3**. Іркуші фаторлар бағасы. Қатердің пайда болуын тоқтататын іркуші фаторлар болып табылатын іркілуші және профилактикалық факторлардың аудиті жүргізіледі. **4**. Қорғаушы, паллативтік және рекуперативтік факторлардың бағасы.

5. Потенциалды баға потенциалды (болуы керек болған) қатер бес балдынша бағаланады: 0 – жоқ; 1 – болуы мүмкін емес; 2 – екіталай; 3 – көбінесе; 4 – болуы ықтимал. **6**. Әсер ету бағасы. Ақпараттық қауіпсіздік-тің іс-шараларына қарамастан қатердің басып алу салдарының бағасы жүргізіледі. **7**. Әсер ету көрсеткіштерінің қысқаруы мен төмендету бойынша шараларды қабылдағаннан кейінгі әсер ету бағасы. **8**. Жаһандық ҚБағ. Ұйымдар үшін жаһандасқан қатерлер айқындалады. **9**. Қатердің қолайлылығы немесе қолайлы еместігі туралы шешім қабылдау. Қатер бағасы мен анализі жүзеге асатын сұраныстар үлгісін қарастырайық – «АҚ менеджерінің қызметтік міндеттерінің яғни мақсаты, қызметі, ақпараттық қауіпсіздік байланысты өзге салалармен өзара әсері айқын анықталғаны бар ма?», «Өз ішіне сезімтал құрал-жабдыққа арналған тоқтаусыз қуат көзін қамтитын электр қуатын беруді реттеуші жүйе бар ма?», «Аудит уақытылы, кем дегенде жылына бір рет жүйедегі мәліметтерді ауыстыру, шифрлау немесе осылармен байланысты процедуралар болып тұра ма?» және т.б. Сонымен бірге әдістемеде әлсіздіктер де қарастырылады, мысалы, бұзылу немесе құрал-жабдықтың істен шығуы қызмет көрсетуге қосылудың үзілуі, программалық файлды ашу, жөнге салуды немесе ПҚұр-ғы шалысуды (қателік) өзгерту мүмкіндігі т.б. [74].

ҚБАҚ 25 - ISO/FDIS 31000 [9] (Risk management – Principles and guidelines (Қатерлерді басқару – негізгі принциптер), Швейцария) **стандарты** қатерді бағалау мен анализдеудің негізгі принциптерін сипаттайды. Мұнда қатерді басқарудың жеті негізгі кезеңдері айқындалған:

1. Ұйым құрылымының және оның мәнмәтінінің сипатталуы;
2. Қатер-менеджмент саясатының анықталуы. Саясат ұйымның мақсатын нақты суреттеуі қажет.
3. Жауапкершіліктің анықталуы;
4. Ұйымдастыру процестерінде интеграция;
5. Ресурстардың идентификациясы;
6. Ішкі байланыстар мен есеп беру механизмдерін жасау;
7. Сыртқы байланыстар мен есеп беру механизмдерін жасау. Бағалауды жүргізу үшін қатер критериялары анықталады, бұл жерде ұйымның мақсаты мен ресурстары суреттелуі, қатер-менеджмент саясатымен қиысуы қажет, қатер-менеджментінің кез келген процесінің басында анықталған және әрқашан қайта қаралады.

Әрі қарай қатер дәрежесін бағалау процесіне өтеді – оның толық идентификациялану, анализдену, бағалану процесі. Идентификация кезеңінде ұйым қатер, әсер ету аясының, оқиғалар және олардың себептерінің, сонымен бірге потенциалды салдардың көзін анықтауы қажет. Анализдеу кезеңінде салдар, ықтималдылық және тағы басқа қатер белгілері анықталады. Бағалаудың мақсаты көбіне анализдеу нәтижесінде шешім қабылдау кезінде көмек көрсетуден тұрады. Қатерді бағалау ҚД критериялармен (мәнмәтінді қарастыру кезінде орнатылған) салыстыруды тұспалдайды [9].

ҚБАҚ 26 - MAGERIT [75] (Methodology for Information Systems Risk Analysis and Management, өңдеуші Ministerio De Administraciones Públicas,

Испания) **әдістеме** қатерді бағалау мен анализдеуді жүзеге асыруға арналған, бұл үш кезеңде өтеді:

0-кезең – Жоспарлау.

1-кезең – Қатер анализі. Бес қадамнан тұрады: 1. Ұйым үшін қажетті АЖ элементтері (немесе олармен тығыс байланысты) болып табылатын белсенділерді анализдеу және идентификациялау. Белсенділерді олардың арасындағы тәуелділіктерді анықтау үшін бес топқа бөлу ұсынылады (қоршаған орта, АЖ, ақпарат, ұйым функциясы, өзге белсенділер). Белсенділерді сараптаудан кейін құнына байланысты оларды бағалау жүргізіледі. Әрі қарай белсендінің шынайылығы мен Қ, Т, ҚЖ-ке талаптар анықталады; 2. Ақпараттық қауіпсіздік ҚБ мен анализдеу. Осы әдістемеде берілген қатер категориясының көмегімен олардың идентификациясы жүргізіледі, жиілік (шкала қолданылады: 100 – өте жиі (күнделікті); 10 – жиі (әр айда); 1 – әдетте (жыл сайын); 1/10 – сирек (бірнеше жылда бір рет) пен шығын бағалауы жүзеге асырылады; 3. Ескертпелі шараларды қауіп-қатерлерді тоқтату үшін анықтау; 4. Әсер ету бағасы. қауіп-қатермен байланысты болған белсенділердің зияндануын өлшеу; 5. Қатерді анықтау. АЖ бұзылу ықтималдығымен қатер әсер етеді де, әсер ету мен жиіліктің өсуімен үлкейеді (1.24-кестесі [75]).

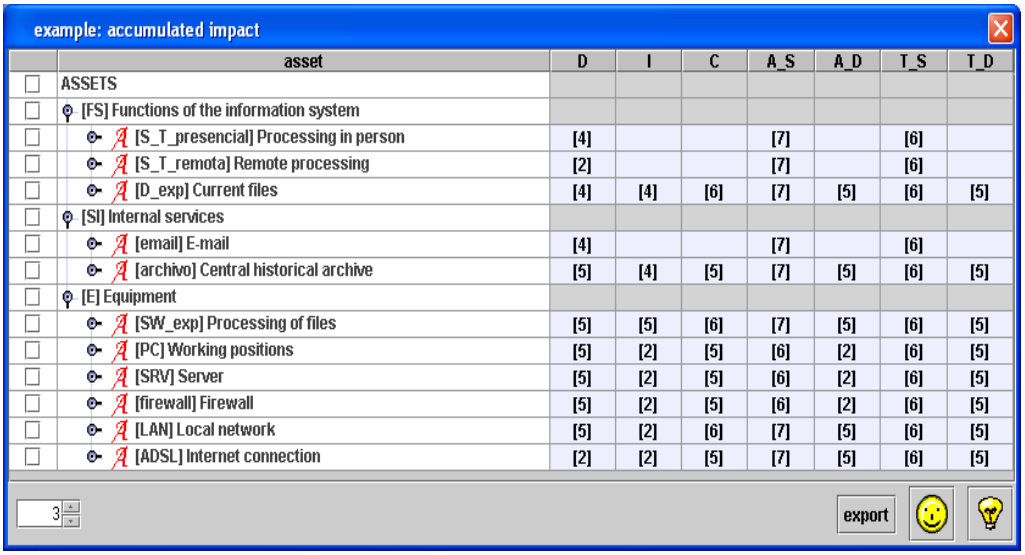
2-кезең – Қатерлерді басқару. Қорғау шаралары (адамдар мен құрал-жабдықтар, ұйымдастырушылық шаралар, кадрлық саясат үшін жұмыс ортасын техникалық, физикалық қорғау) таңдалады және жүзеге асырылады, сонымен бірге қалдық қатерлер мен әсер ету үшін мән интерпретациясы жүзеге асырылады, шығындалу мен пайдалану анализі жүргізіледі [75].

Кесте 1.25 - Файлды мәліметтерге потенциалды қауіп-қатер үлгісі

Ақпараттық қауіпсіздік өлшеу (%)								
белсенді/қауіп-қатер	F	D	I	C	AS	AD	TS	TD
[D_exp] Ағындағы файлдар		50	50	100	100	100	100	100
[E.1] Тұтынушылар қателері	10	10	10					
[E.2]Әкімшінің қателіктері	1	20	20	10	10	10	20	20
[E.3] Мониторинг қателіктері	1						50	50
[E.4] Кескіндеме қателіктері	0,5	50	10	10	50	50	50	50
[E.14] Ақпараттың жайылып кетуі	1			1				
[E.15] Бұрмаланған ақпарат	10		1					
[E.16] Қате мәліметтердің енгізілуі	100		1					
[E.18] Ақпараттың жойылуы	10	1						
[E.19] Ақпараттың ашылуы	1			10				
[A.4] Кескіндеменің өзгеруі	0,1	50	10	50	100	100	100	100
[A.11] Рұқсат етілмеген мүмкіндік	100		10	50	50			

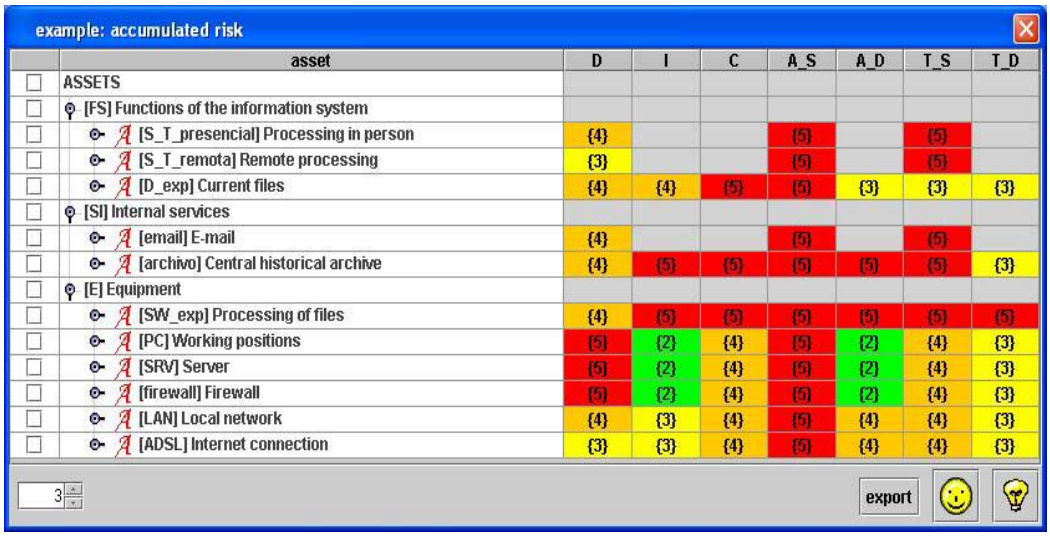
Әдістеме «Techniques Guide» Ақпараттық қамтамасыздандыруында жүзеге асырылған, бағалау үлгілері 1.19 және 1.20 суреттерінде көрсетілген, мұндағы D, I және C – оған сәйкесінше мәліметтердің Қ, Т пен ҚЖ, AS мен AD – сәйкесінше қолданушы қызметтің шынайылығы мен мәліметтерді өту, TS мен TD –

сәйкесінше мәліметтерге қол жетімділік пен қызметті қолданудың есеп беру міндеті [75].



asset	D	I	C	A_S	A_D	T_S	T_D
ASSETS							
[FS] Functions of the information system							
[S_T_presencial] Processing in person	[4]			[7]		[6]	
[S_T_remota] Remote processing	[2]			[7]		[6]	
[D_exp] Current files	[4]	[4]	[6]	[7]	[5]	[6]	[5]
[SI] Internal services							
[email] E-mail	[4]			[7]		[6]	
[archivo] Central historical archive	[5]	[4]	[5]	[7]	[5]	[6]	[5]
[E] Equipment							
[SW_exp] Processing of files	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC] Working positions	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[SRV] Server	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[firewall] Firewall	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[LAN] Local network	[5]	[2]	[6]	[7]	[5]	[6]	[5]
[ADSL] Internet connection	[2]	[2]	[5]	[7]	[5]	[6]	[5]

Сурет 1.19 - Әсер ету бағасының үлгісі



asset	D	I	C	A_S	A_D	T_S	T_D
ASSETS							
[FS] Functions of the information system							
[S_T_presencial] Processing in person	{4}			{5}		{5}	
[S_T_remota] Remote processing	{3}			{5}		{5}	
[D_exp] Current files	{4}	{4}	{5}	{5}	{3}	{3}	{3}
[SI] Internal services							
[email] E-mail	{4}			{5}		{5}	
[archivo] Central historical archive	{4}	{5}	{5}	{5}	{5}	{5}	{3}
[E] Equipment							
[SW_exp] Processing of files	{4}	{5}	{5}	{5}	{5}	{5}	{5}
[PC] Working positions	{5}	{2}	{4}	{5}	{2}	{4}	{3}
[SRV] Server	{5}	{2}	{4}	{5}	{2}	{4}	{3}
[firewall] Firewall	{5}	{2}	{4}	{5}	{2}	{4}	{3}
[LAN] Local network	{4}	{3}	{4}	{5}	{4}	{4}	{3}
[ADSL] Internet connection	{3}	{3}	{4}	{5}	{4}	{4}	{3}

Сурет 1.20 - Қатер бағасының үлгісі

ҚБАҚ 27 – Information SecurityRA [76] (Risk Assessment, өңдеуші Centers for Medicare & Medicaid Services (CMS), АҚШ) **әдістемесі** ақпараттық қауіпсіздік саласында АОР жүзеге асыру мүмкіндігін береді. Әдістеме үш сатыдан тұрады:

1-саты. Жүйені құжаттандыру. Саты бірнеше процесте жүзеге асырылады – белсенділер мен жүйелік құжаттардың идентификациясы, сонымен бірге ақпараттық қауіпсіздіктің ағындағы деңгейін анықтау (шкалаларын қолданумен: «Ж», «О» және «Т» 1.26 -кестесінде [76]); 2-саты. Қатерді анықтау. Қ, Т пен ҚЖ зақымдану көзқарасы жағынан АЖ-ге (оның мәліметтері мен бизнес-функциялар) әсер ететін әлсіздікті қолданған қатер мен әсер ету

дәрежесінің жүзеге асырылу ықтималдығы негізінде әрбір қауіп-қатер мен әлсіздіктер жұбына ҚД есептеу.

2-саты 6 қадамнан тұрады: 1. Қауіп-қатерді айқындау; 2. Әлсіздікті айқындау; 3. Берілген қауіп-қатерді (әлсіздікті қолданумен) жүзеге асыру қатерін төмендету үшін бар болған басқару элементтерін айқындау. 4. Жеті деңгейлі шкала қолданылып отырған басқару элементтерін есепке ала отырып оның ПБЫ анықтау: МЕ – маңызды емес (екіталай); ӨТ – өте төмен (мүмкін бес жылда екі/үш рет); Т – төмен (жылына бір рет немесе оннан да аз); О – орташа (алты айда бір рет болуы мүмкін немесе онан да аз); Ж – жоғары (айда бір рет болуы мүмкін немесе оннан да аз); ӨЖ – өте жоғары ықтималдылық (бір айда бірнеше рет); ЭТЫ – Экстремалды түрде ықтимал (күніге бірнеше рет). 5. Жүйеге әсер ету дәрежесін бағалау жеті деңгейлі шкала бойынша жүзеге асырылады: МЕ – маңызды емес, АЗ – азғантай, АЙ – айтарлықтай, БҰ – бұзатын, МА – маңызды, ӨҚ – өте қиын. 6. Бар болған басқару элементтерінің қауіп-қатер мен әлсіздік жұбы үшін ҚД анықтау. Қатер дәрежесі 1.26-кестесіне сай анықталады [76].

Кесте 1.26 - Қатер деңгейлері

ПБЫ	Әсер ету					
	МЕ	АЗ	АЙ	БҰ	МА	ӨҚ
МЕ	Т	Т	Т	Т	Т	Т
ӨТ	Т	Т	Т	Т	О	О
Т	Т	Т	О	О	Ж	Ж
О	Т	Т	О	Ж	Ж	Ж
Ж	Т	О	Ж	Ж	Ж	Ж
ӨЖ	Т	О	Ж	Ж	Ж	Ж
ЭТЫ	Т	О	Ж	Ж	Ж	Ж

3-саты Қорғауды анықтау төрт қадамнан тұрады: 1. Қауіп қатерді төмендету үшін басқару/шаралар қауіпсіздік элементтерін анықтау; 2. Қауіптің қалдық ықтималдығын анықтау; 3. Әлсіздіктің қалдық әсерлерді анықтау; 4. Жүйедегі қалдық қатерлер деңгейін анықтау.

Бірінші бөлім бойынша тұжырым

1. Қатермен байланысты қор түсінігі зерттелді және анализденді. Жүргізілген анализ қатердің әртүрлі тұжырымдалуы ортақ жиынтық сипаттамасына ие екенін көрсетеді, мысалы, қатердің ықтималдықпен және белгілі бір оқиғаның басталуымен т.б. байланысы. Ақпараттық қауіпсіздік саласында бұл түсінікті түсіндіру үшін осы салаға қатысты оның сипаттама қор жиынтығын ерекшелеу қажет.

2. Ақпараттық қорғаудың тапсырмаларына сәйкесінше шешетін тиімді аспапты жасау мен таңдау үшін қолданылатын кіріс, ішкі және сыртқы параметрлерді анықтау мақсатында бар болған стандарттарды, әдістерді,

әдістемелерді, әдіснамаларды және программалық ҚБАҚ зерттеу мен анализдеу жүргізілді.

2 АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРІН БАҒАЛАУ МЕН АНАЛИЗДЕУДІҢ ӘДІСТЕРІ МЕН МОДЕЛЬДЕРІ

2.1 Қауіптің сипаттама қорының кортежді моделі

Кәсіпорын IT-инфрақұрылымының қарқынды өсуі ақпараттық ресурстардың әлсіздігі және ақпараттыық қауіп-қатер санының бақыланбайтын өсуіне алып келеді. Мұндай жағдайларда ақпараттық қауіпсіздік қатерін бағалау ақпаратты қорғаудың қажетті деңгейін анықтауға, оны қолдауды жүзеге асыруға және компанияның ақпараттық құрылымының даму стратегиясын өңдеуге мүмкіндік береді. Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу бизнесті жаңарту мен үздіксіздікті қамтамасыз ететін жоспарды және қатерлерді басқару жүйесін жасауда қажетті шарттылық болып табылады.

Бүгінгі күні қатерді бағалау мен анализдеу әдістемесінде бірігетін көптеген аспаптық құралдар бар. Бұл әдістер нормативті құжаттармен (стандарттармен) басталып, нақты программалық заттармен аяқталатын айтарлықтай кең спектрде беріледі. Ақпаратты қорғау мәселесін шешудің тиімділігін арттыру үшін компания мамандарының алдында адекватты талаптарды қанағаттандырып, сәйкес келетін әдісті таңдау туралы сұрақ туындайды. Мұндаай таңдауды жүзеге асыру алдында ақпараттық қауіпсіздік аспектісінде қатер түсінігін айтарлықтай толық елестету қажет болады.

1.1 п. Оны ақпараттық қауіпсіздік саласында елестету мақсатында адам қызметінің көптеген салаларында қатер түсінігіне талдау жүргізілді, сонымен бірге қатердің сипаттама қоры көрсетілді.

Әр түрлі баспаларда айтарлықтай кең түсіндірмеге ие қатердің әр түрлі анықтамалары бар. Тек қана Ғаламтор-сөздігінің өзінде көптеген адам қызметінің салаларымен байланысты 1500-ден астам қатер түсінігі бар. Осының салдарынан қатердің өзінің және оның түсініктерімен байланысты болмысын ашуыға қатысты әр түрлі мағынасыздықтар пайда болады. Сәйкесінше мұндай жағдай ақпараттар қауіпсіздігінің саласына да тән болмақ.

Қатердің әр түрлі пәнаралық салаларды қамтуын есепке ала отырып, бұл түсінікті мынадай көзқарастар жағынан қарастыру қажет:

- қауіпсіздік,
- психология,
- экономика,
- сақтандыру,
- медицина,
- геология

т.б., бұлар монографияларда, статьяларда, оқулықтарда, сөздіктерде, сонымен бірге халықаралық, ұлттық және ұлттық құжаттар сияқты әр түрлі нормативтерде кездеседі.

Қатер сипаттама қорын қалыптастыру процесін рәсімдеу үшін мүмкін болған сипаттама жинағын енгіземіз [77, 78].

$$\boldsymbol{BC} = \bigcup_{i=1}^{n} \boldsymbol{BC}_i = \{\boldsymbol{BC_1}, \boldsymbol{BC_2}, ..., \boldsymbol{BC_n}\},$$

Мысалы, n=6 кезінде $\boldsymbol{BC}$ жиынтық мынадай түрге ие болуы мүмкін

$$\boldsymbol{BC} = \bigcup_{i=1}^{6} \boldsymbol{BC}_i = \{\boldsymbol{BC_1}, \boldsymbol{BC_2}, \boldsymbol{BC_3}, \boldsymbol{BC_4}, \boldsymbol{BC_5}, \boldsymbol{BC_6}\} =$$

{«**Әрекет**», «**Оқиға**», «**Ықтималдылық**», «**Қатер**», «**Жиілік**», **Шығындар**»}.

Адам қызметінің әр түрлі салаларында қауіп түсінігінің талдауы жүргізілгеннен кейін қатердің келесі сипаттама қорын ерекше көрсетуге болады- ақпараттық қауіпсіздік оқиғасының бұзылуына алып келген **«Әрекет» ($\boldsymbol{BC_1}$).** Ақпараттық қауіпсіздік көзқарасы жағынан $\boldsymbol{BC_2}$ жағымсыз оқиғалардың туындауына алып келген ақпараттық жүйе ресурстар (АЖР) қауіпсіздігінің сипаттама қорынын потенциалды **қауіп-қатерді** жүзеге асырумен байланысты. Осыған байланысты $\boldsymbol{BC_1}$ базалық сипаттамасын

$$\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i} = \{BC_{11}, BC_{12}, ..., BC_{1bc_1}\},$$

идентификаторлар жиынтығымен беруге болады, (мұндағы bc_1 – қатердің идентификаторлар саны), мысалы, bc_1=3 кезінде $\boldsymbol{BC_1}$ жиынтығы мына

түрге $\boldsymbol{BC_1} = \bigcup_{i=1}^{3} BC_{1i} = \{BC_{11}, BC_{12}, BC_{13}\} =$ {«Компьютерлік тыңшылық», «Тыңшылық», «Программалық қамтамасыздандырудың шалысуы»} ие болады.

Келесі сипаттама қорын белгі айнымалысы түрінде бейнелеуге болатын **«Оқиға» ($\boldsymbol{BC_2}$)** түрінде анықтауға болады болатын соңғы идентификаторлар $\boldsymbol{BC_2} = \bigcup_{i=1}^{bc_2} BC_{2i} = \{BC_{21}, BC_{22}, ..., BC_{2bc_2}\}$ (bc_2 – оқиғалар идентификаторларының саны) жиынтығының бір мәнін қабылдаушы нышан айнымалысы түрінде беруге болады.

Ақпараттық қауіпсіздік саласында қатер құпиялылық, тұтастық пен қол жетімділік сияқты ақпараттық жүйе ресурстарының (АЖР) қауіпсіздік сипаттамалар қорымен байланыстылылығын есепке ала отырсақ, онда bc_5=7 кезінде қор оқиғалары

$\boldsymbol{BC_2} = \bigcup_{i=1}^{7} BC_{2i} = \{BC_{21}, BC_{22}, BC_{23}, BC_{24}, BC_{25}, BC_{26}, BC_{27}\}$ = {«Құпиялылықтың бұзылуы (ҚБ)», «Тұтастықтың бұзылуы (ТБ)», «Қол жетімділіктің бұзылуы (ҚжБ)», « Құпиялылық пен тұтастықтың бұзылуы (ҚТБ)», «Қол жетімділік пен тұтастықтың бұзылуы (ҚжТБ)», «Қол жетімділік пен құпиялылықтың бұзылуы (ҚжҚБ)», «Қол жетімділік, тұтастық пен құпиялылықтың бұзылуы (ҚжТҚБ)»} түрінде идентификациялануы мүмкін.

Айта кететін жайттардың бірі, статистикалық мәліметтерді алуда қиындық туындағанда, сонымен бірге, көлем интерпритациясының қарапайымдылығы үшін сарапшылар логика-лингвистикалық тәсілді қолданады. Оның көмегімен «**Ықтималдылық**» белгілі бір анықталған базалық терм-жиынтықты, мысалы,

$$\boldsymbol{BC_3} = \bigcup_{i=1}^{bc_3} \underset{\sim}{BC}_{3i}$$

(bc_3 – термдер саны), мұндағы мүшелерге тәртіп қатынасы $\underset{\sim}{BC}_{31} < \underset{\sim}{BC}_{32} < ... < \underset{\sim}{BC}_{3bc_3}$ әділ, лингвистикалық айнымалы (ЛА) арқылы [77, 78] сәйкес келетін сипаттама берілуімен жүзеге асырылады. Айта кетсек, $\boldsymbol{BC_3}$ лингвистикалық айнымалы термдері нақты емес сандарды салыстыру әдісін қолдану арқылы көрсетілген қатынаспен байланысады [77, 78]. Мысалы, берілген логикалық айнымалы үшін $\underset{\sim}{T}, \underset{\sim}{O}$ және $\underset{\sim}{Ж}$, нақты емес сандарымен берілетін және сәйкесінше «төмен» (Т), «орташа» (О) және «жоғары» (Ж) лингвистикалық эквивалентіне ие $\boldsymbol{BC_3} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{3i} \{\underset{\sim}{BC}_{31}, \underset{\sim}{BC}_{32}, \underset{\sim}{BC}_{33}\} = \{\underset{\sim}{T}, \underset{\sim}{O}, \underset{\sim}{Ж}\}$ термдер жиынтығын қалыптастыруға болады. Болашақта атақты әдістер [77, 78] негізінде көрсетілген нақты емес сандар үшін қажетті тиістілік функциясы (ТФ) қалыптасады. Сонымен бірге бұдан да басқа термдердің бастапқы мәндері де енгізілуі мүмкін, мысалы, «өте төмен» (ӨТ), «орташадан жоғарылау» (ОЖ), «Орташадан төмен» (ОТ) және т.б. Көзге көрініп тұрғандай, $\boldsymbol{BC_3}$ сипаттамасы мұндай жағдайда лингвистикалық мәндерді терумен беріледі, бірақ тек жеке жағдайда, ол нақты немесе интервалды мән қабылдауы мүмкін, онда оның берілуі үшін жартылай қара жазуды қолданамыз, мысалы, BC_3.

Сонымен бірге, қатердің және бір сипатама қорын яғни **қауіптілікті ($\boldsymbol{BC_4}$)** анықтайық. Ол ақпараттық қауіпсіздік оқиғасының бұзылу қауіптілігімен сипатталатын шама түрінде қарастырастырылады, мысалы, BC_{12} арқылы BC_{21}. $\boldsymbol{BC_3}$ аналогиясы бойынша $\boldsymbol{BC_4}$ сипаттама қоры нақты санды формада (мысалы, пайызда) беріледі де, BC_4 түрінде белгіленеді немесе лингвистикалық айнымалы көмегімен – «**Қауіптілік**» базалық терм-жиынтықпен

$$\boldsymbol{BC_4} = \bigcup_{i=1}^{bc_4} \underset{\sim}{BC}_{4i} \ (\underset{\sim}{BC}_{41} < \underset{\sim}{BC}_{42} < ... < \underset{\sim}{BC}_{4bc_4})$$

белгіленеді.

Мысалы, bc_4=3 болса, «төмен» (Т), «орташа» (О) және «жоғары» (Ж) лингвистикалық эквиваленттері бар $\boldsymbol{BC_4} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{4i} = \{\underset{\sim}{BC}_{41}, \underset{\sim}{BC}_{42}, \underset{\sim}{BC}_{43}\} = \{\underset{\sim}{T}, \underset{\sim}{O}, \underset{\sim}{Ж}\}$ анықтауға болады.

Жоғарыда көрсетілген қатер талқылауларының жиынтығынан мынадай сипаттамалар қорын ерекшелеуге болады: Ақпараттық қауіпсіздіктің бұзылуына алып келген, ақпараттық қауіпсіздік саласында «қауіп-қатерді» жүзеге асыру жиілігімен байланыстыруға болатын ($\boldsymbol{BC_5}$) **жиілігін** алуға болады. Мұндай компонентті (BC_5) санды немесе лингвистикалық айнымалы - **«Жиілік»** арқылы беруге болады:

$$\boldsymbol{BC_5} = \bigcup_{i=1}^{bc_5} \underset{\sim}{BC}_{5i} \ (\underset{\sim}{BC}_{51} < \underset{\sim}{BC}_{52} < ... < \underset{\sim}{BC}_{5bc_5}),$$

мысалы, егер bc_5=3 болса, онда $\boldsymbol{BC_5} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{5i} = \{\underset{\sim}{BC}_{51}, \underset{\sim}{BC}_{52}, \underset{\sim}{BC}_{53}\} = \{\underset{\sim}{T}, \underset{\sim}{O}, \underset{\sim}{Ж}\}$, мұндағы $\underset{\sim}{T}, \underset{\sim}{O}$ мен $\underset{\sim}{Ж}$ сәйкесінше «төменгі» (Т) «орташа» (О) «Жоғары» (Ж) - лингвистикалық эквиваленті.

Ақпараттық қауіпсіздік саласында **($\boldsymbol{BC_6}$) шығын** терминдері арқылы мақсатқа сай анықтайтын **шығын мен зақымданудың** сипаттама қорын және (BC_6) сандық жағынан ұсынуды анықтап алайық мысалы, қойылған интервалдарда

1) 0 - $100;
2) $100 - $1000;
3) $1000 - $10 000;
4) $10 000 - $100 000.

Сонымен бірге $\boldsymbol{BC_6}$ «**Шығындар**» **лингвистикалық айнымалы көмегімен анықтауға болады:**

$$\boldsymbol{BC_6} = \bigcup_{i=1}^{bc_6} \underset{\sim}{BC}_{6i} \ (\underset{\sim}{BC}_{61} < \underset{\sim}{BC}_{62} < ... < \underset{\sim}{BC}_{6bc_6}),$$

мұндағы, мысалы, bc_6=5 болса, лингвистикалық айнымалы $\boldsymbol{BC_6} = \bigcup_{i=1}^{5} \underset{\sim}{BC}_{6i} =$

$\{\underset{\sim}{BC}_{61}, \underset{\sim}{BC}_{62}, \underset{\sim}{BC}_{63}, \underset{\sim}{BC}_{64}, \underset{\sim}{BC}_{65}\} = \{\underset{\sim}{T}, \underset{\sim}{OT}, \underset{\sim}{O}, \underset{\sim}{OЖ}, \underset{\sim}{Ж}\}$ түріне ие болады , ал нақты емес сандар қолданылып жатқан лингвистикалық эквиваленттер сәйкесінше «төмен» (Т), «орташадан төмен» (ОТ), «орташалар» (О), «Орташадан жоғары» (ОЖ) және «жоғары» (Ж). Практикада интеграцияланған $\boldsymbol{BC_6}$ ұсынысы да кездеседі, мысалы, 1) *Negligible* ($100-дан кем);
2) *Minor* ($1000кем);
3) *Moderate* ($10 000 кем);
4) *Serious* (бизнеске айтарлықтай жағымсыз әсер етеді);
5) *Critical* (Апаттық әсер, мекеме қызметінің тоқтауы мүмкін) [56].

Мұндай жағдайда сипаттамалар BC_6 / $\boldsymbol{BC_6}$ түрінде белгіленеді. Зерттеліп жатқан қауіп талқылаулар жиынтығы үшін оның базалық сипаттамасы бөлінген еді: қауіп өлшенетін немесе есептеп шығаратын ықтималдылық түрінде қаралады; қауіп белгілі бір оқиғаның басталуымен байланысты (әдеттегідей, сәтсіз); қауіп түсінігі субъект қызметі арқылы ашылады; қауіп субъекті қызметіне тәуелсіз түрде болып жатқан оқиға арқылы ашылады; қауіп шығын, жоғалту, қауіптілік түрінде қабылданады.

Жалпылау түрінде ақпараттық қауіпсіздік сферасында берілген қауіптің сипаттама қорының интеграцияланғандығын қолдану үшін оларды *m*-компонентті $< \boldsymbol{BC_1, BC_2, ..., BC_m} >$ кортеж қоры моделі түрінде таныстыру ұсынылады, мұндағы m ($m \leq n$) – кортеждегі мүшелер саны. Мысалы, m=6 болғанда алты компонентті кортеж мынадай түрге ие болуы мүмкін:

$$\boldsymbol{<BC_1, BC_2, BC_3, BC_4, BC_5, BC_6>,}$$

мұндағы $\boldsymbol{BC_1}$ – әрекет, $\boldsymbol{BC_2}$ – оқиға, $\boldsymbol{BC_3}$ – ықтималдылық, $\boldsymbol{BC_4}$ – қауіптілік, $\boldsymbol{BC_5}$ – жиілік, $\boldsymbol{BC_6}$ – шығындалу мен жоғалулар (шығындар). Қолданылып жатқан сипаттамалардың нақтылығының нәтижесінде жеке кортежді модель пайда болады, мысалы, BC_{12} = «Тыңшылық» үшін, BC_{22} = «НК», bc_3=3, bc_4=3, bc_5=3 және bc_6=5 мына түрге ие болады: $<BC_{12}, BC_{21}, \boldsymbol{BC_3}, \boldsymbol{BC_4}, \boldsymbol{BC_5}, \boldsymbol{BC_6}> = <BC_{12}, BC_{21}, \bigcup_{i=1}^{3} \underset{\sim}{BC}_{3i}, \bigcup_{i=1}^{3} \underset{\sim}{BC}_{4i}, \bigcup_{i=1}^{3} \underset{\sim}{BC}_{5i}, \bigcup_{i=1}^{5} \underset{\sim}{BC}_{6i}>$.

Көрініп тұрғандай егер базалық шамалар нақты немесе нақты емес мәндерге ие болса, онда жеке кортежде (жеке кортежді модельде) олар сәйкесінше қанық қара жазумен немесе қанық емес жазумен белгіленеді, мысалы, BC_{12}, BC_{21} немесе $\boldsymbol{BC_3}$, $\boldsymbol{BC_4}$, $\boldsymbol{BC_5}$, $\boldsymbol{BC_6}$.

Ұсынылған кортежді модель негізінде қауіпті бағалау мен бар болған анализ құралдарының кең ауқымды спектрін бастапқы мәліметтердің жұмыс істеуі үшін қажетті қалыптастыру позициясы жағынан зерттеуді жүзеге асыруға болады, бұл жаңа жүйені жасауға амал анықтауға немесе қолда барын ақпараттық қорғау мәселелеріне сәйкесінше тиімді шешім қабылдау мақсатында қолдануға мүмкіндік береді.

2.2 Қатерді бағалау мен анализдеу құралдарында қолданылатын сипаттама қоры

Бүгінгі күні (ҚБАҚ) қауіпті бағалау мен анализдің аспаптардың айтарлықтай кең жиынтығы бар. Компания мамандарының алдында ақпаратты қорғау (АҚор) мәселесін тиімді шешуді жоғарылату үшін сәйкес келетін, адекватты талаптарды қанағаттандыратын әдістемені таңдау туралы жиі сұрақ туындайды. 1.1. п ақпараттық қауіпсіздік (АҚ) саласындағы, оның кезектегі интерпретациясы үшін адам қызметінің әр түрлі пәнаралық салаларында қауіп түсінігінің анализі жүзеге асырылған. Сонымен бірге 2.1 п. қауіптің сипаттама қорының кортежді моделі (ҚКМ) жалғасқан болатын. Мұндай тәсіл, ҚКМ қатысты бар болған ҚБАҚ зерттеу процесін біріңғайластыруға және оларды тиімді таңдауды жоғарылатуға мүмкіндік береді. Сонымен бірге, сәйкес келетін анализ жүзеге асырылмағандықтан қатер сипаттамасының жиынтығы анықталмаған бұдан басқа да көптеген осы сияқты құралдар бар.

Осыған байланысты, берілген жұмыстың мақсаты бар болған ҚБАҚ-ның жиынтық сипаттамасын (2.1. п. ұсынылғанды қолданумен) анықтау үшін, осындай құралдардың салыстырмалы анализін жүзеге асыруға болатын, онда кең спектрлі зерттелу жүргізілді. Бұл АҚ саласындағы мәселелерді тиімді шешуді жоғарылатады.

Зерттеудің бастапқы материалы түрінде көптеген белгілі және тәжірибеде қолданылып жүрген ҚБАҚ – COBRA, CRAMM, RiskWatch, RA2 art of risk (RA Software Tool), АҚ басқару КЭЖ «АванГард» («ҚатерМенеджері»), Risk Advisor, vsRisk, OCTAVE, Callio Secura 17799, Гриф 2006, @RISK, RiskPAC және Microsoft Security Assessment Tool, байесті желілер негізінде әдіс, NIST 800-30, VAR, TRA, FRAP, BSI-Standard 100-3, РС БР ИББС-2.2-2009, ISO/IEC

27005, Risk Matrix, AS/NZS 4360:2004, Mehari, ISO/FDIS 31000, MAGERIT, Information Security RA көбісі алынған болатын.

ҚБАҚ 1 - NIST 800-30 (Risk Management Guide for Information Technology Systems, NIST ұсынысы, өңдеуші – National Institute of Standards and Technology, АҚШ**) [70].**

ҚКМ қатысты осы әдіснама үшін кортежді анықтайық. BC_1 сипаттамасы «Қауіп-қатер әрекетімен» (1.1-кестесін қара) беріледі, бұл өз кезегінде АҚ сипаттамасының бұзылуына алып келуі мүмкін, мысалы, BC_{11}=«жеке мәліметтер негізінде АЖ-ге ену» BC_{21}=«ҚБұзылуына» алып келуі мүмкін. ҚД бағалау үшін әдіснамада «Әсер ету» параметріндегі мәнді көрсететін BC_3 сипаттама қоры және жанама BC_4^* қолданылады (2.1-кестеге қара). Сәйкесінше, әдіснама үшін кортеж мына түрге ие: $< BC_1, BC_2^*, BC_3, BC_4^* >$.

Кесте 2.1 - Қауіп деңгейінің матрицасы

Қауіп-қатер ықтималдығы	Әсер етуі		
	Т (10)	*О (50)*	*Ж (100)*
Ж (1,0)	**Т** 10 × 1,0 = 10	**О** 50 × 1,0 = 50	**Ж** 100 × 1,0 = 100
О (0,5)	**Т** 10 × 0,5 = 5	**О** 50 × 0,5 = 25	**О** 100 × 0,5 = 50
Т (0,1)	**Т** 10 × 0,1 = 1	**Т** 50 × 0,1 = 5	**Т** 100 × 0,1 = 10

ҚБАҚ 2 - BSI-Standard 100-3 әдістемесі (Risk Analysis based on IT-Grundschutz – IT-Grundschutz негізінде қауіп анализдері, ақпараттық қауіпсіздікіпсіздік бойынша Федеральды Агенттігімен өңделген (Federal Office for Information Security – BSI), Германия) [72].

ҚКМ есепке ала отырып, айта кететін жайт, (BC_1) барлық әрекеттер жиынтығы АҚ-тің бұзылуына алып келетін қауіп-қатер түрінде берілген, мысалы, BC_{11}=«IT жүйесінің істен шығуы», BC_{12}=«Белсендіні абайсызда жою», BC_{13}=«Ақпараттың Т жоғалуы» мен т.б. BC_2 сипаттамасына қатысты, айта кететін жайт, қаралған әрекеттер АҚ-ң белгілі бір сипаттамаларының (1.5-кестеде берілген үлгі бойынша) бұзылуына алып келеді де, BC_{27}=«ҚТҚЖБ» мәнімен жанама байланысқан болуы да мүмкін. ҚКМ есепке ала отырып, кортежді осы әдістеме үшін мынадай түрде ұсынуға болады: $<BC_1, BC_2>$.

ҚБАҚ 3 - РС БР ИББС-2.2-2009 әдістемесі (Ресей банк стандарттау саласындағы ұсыныстар, банктік жүйесіндегі ұйымдардың ақпараттық қауіпсіздігін қамтамасыз ету Ресей Федерациясы) [64].

Айта кететін жайт, АҚ бұзылуына алып келетін ҚБАҚ-да қауіп-қатерлер (BC_1) әрекет түрінде бейнеленеді, мысалы, (ұсынылып отырған тізімдегі қауіп-қатер әдістемеде – Қосымша 1 [62]), BC_{11}= «ПҚ істен шығуы мен бас тартуы», BC_{12}=«Өмірлік цикл сатысындағы АЖ қауіпсіздігін қамтамасыз етудегі қателер», BC_{13}=«Сақтау орны» т.б. Мысалдағы қаралған (BC_1) әрекет АҚ сипаттама қорының бұзылу (BC_2) оқиғаларымен байланысты болуы мүмкін, мысалы, BC_{11} с BC_{23}=«ҚЖБ», BC_{12} с BC_{27}=«ҚЖТҚБ», ал BC_{13} с BC_{21}=«ҚБ» т.б.,

сондықтан BC_2^* сипаттамасы әдістемеде жанама түрінде бар. Басқа сипаттамаларға келсек, мұнда қатерді бағалау кезінде Сап шкалаларында BC_4 (Сан ауыстыруы кезіндегі шкалалар – BC_6), сонымен бірге, (BC_3) ықтималдығы мен (BC_5) қауіп-қатерді жүзеге асыру жиілігі туралы статистикалық мәліметтер көмегімен жанама көрсетуге болатын потенциалды шығын дәрежесі қолданылады. Жүргізілген анализден соң, ҚКМ есепке ала отырып, осы әдістеме үшін кортеж төмендегідей: $<BC_1, BC_2^*, BC_3, BC_4, BC_5, BC_6>$.

ҚБАҚ 4 - ISO/IEC 27005:2008 стандарты (Information technology – Security techniques – Information security risk management (Ақпараттық технология – Қорғаныс әдістері – АҚ қатерінің менеджменті) ISO/IEC TR 13335-3:1998 мен ISO/IEC TR 13335-4:2000 стандарттарды техникалық тұрғыдан қайта қарастырады яғни өзгерту мен ауыстыру, Швейцария) [4].

Айта кететін жайт, ISO/IEC 27005:2008-да қатер түрінде ақпараттық қауіпсіздік бұзылуына алып келетін әрекет қарастырылады, мысалы, BC_{11}=«Тасушылар мен құжаттардың ұрлануы» BC_{21}=«ҚБ» логикалық байланыста болуы мүмкін, сондықтан BC_2^* сипаттамасы стандартта жанама кездеседі. Қатерді бағалау мен анализдеу кезінде BC_3 компонентін қосымша және BC_4^* (потенциалды салдар көлемі) – жанама идентификациялауға болады, сондықтан кортеж мына түрге ие: $<BC_1, BC_2^*, BC_3, BC_4^*>$.

ҚБАҚ 5 - AS/NZS 4360:2004 стандарты (Австралия мен Жаңа Зеландия қатер-менеджмент стандарты) [65].

Берілген стандартты ҚКМ қатысты қарастырайық. Демек, BC_1 сипаттамасына қатерге алып келуі мүмкін әрекеттер сәйкес келеді (1.16-кестесінен көрініп тұрғандай). Сондықтан оларды мысалы, BC_{11}=«Жүйенің істен шығуы» (1.17-кестесінде жазылған салдардан шыға алынған үлгі) түрінде елестетуге болады, бұл АҚ шабуыл жасалған ресурстар сипаттамасының бұзылуына алып келіп, BC_{25}=«ТҚЖБ» мәнімен байланысты болуы мүмкін. Қатерді бағалау кезінде (BC_4) қауіптілік деңгейі түрінде түсіндіруге болатын (BC_3) қауіп-қатер ықтималдығы мен әсер етуі анықталады. Жүргізілген талдау көрсеткендей кортеж берілген стандарт үшін мынадай түрге ие: $<BC_1, BC_2^*, BC_3, BC_4^*>$.

ҚБАҚ 6 - ISO/FDIS 31000 стандарты (Risk management – Principles and guidelines (Қатерді басқару – басқару принциптері), Швейцария) [71].

ҚКМ қатысты стандартта АҚ бұзылуына алып келетін (BC_1) әрекеті түрінде беруге болатын қатер оқиғасы қаралуын айта кетейік, мысалы BC_{11}=«Хакердің шабуылынан веб-сервер қызметінен бас тарту», BC_{12}=«Шамадан артқандықтан криптосервердің төмендеуі», BC_{13}=«Тұтынушы құпия сөздерін басып алу» т.б. Бұл әрекеттер сәйкесінше АҚ BC_{23}=«ҚЖБ», BC_{27}=«ҚТҚЖБ», BC_{21}=«ҚБ» т.б., сипаттама қоры бұзылуының (BC_2) оқиғаларымен байланысты, сондықтан BC_1^* және BC_2^* сипаттамалары стандартта жанама болады. қатерді талдау барысында сипаттамалар (BC_3) қатер ықтималдығы мен BC_4 арқылы бейнелеуге болатын әсер ету болып

елестетіледі. ҚКМ есепке ала отырып, талдауды жүргізген соң стандарт үшін кортеж мынадай болады: $<\boldsymbol{BC_1^*}, \boldsymbol{BC_2^*}, \boldsymbol{BC_3}, \boldsymbol{BC_4^*}>$.

ҚБАҚ 7 - COBRA (Consultative Objective and Bi-Functional Risk Analysis, өңдеуші – C & A Systems Security Ltd**,** Ұлыбритания) **әдістемесі** [60, 61].

COBRA әдістемесі үшін қатердің сипаттама қорына қатысты (2.1. п. қара) мына сияқты кескіндерді алуға болады: $\boldsymbol{BC_1}$**,** $\boldsymbol{BC_2}$. Міне осылай, $\boldsymbol{BC_1}$ компонентіне (берілген мысалға байланысты) мысалы, BC_{11} = «Ұрлық» мәні сай келеді. Бұл әрекет шабуыл жасалған ресурстардың қауіпсіздік сипаттамасының белгілі бір бұзылуына алып келіп, BC_{27}=«ҚТҚЖБ» мәнімен байланысты болуы мүмкін.

Айта кететін жайттардың бірі, талданушы әдістемеде қатер үш сипаттама қорымен беріледі, олардың бастапқысы мен ең соңғысы өз ішінде $\boldsymbol{BC_1}$ **және** $\boldsymbol{BC_2}$ алып жүр. Проценттер түрінде берілген (қатердің басталу ықтималдығы), «ҚАТЕР ДЕҢГЕЙІНЕ» сай келетін $\boldsymbol{BC_1}$ **және** $\boldsymbol{BC_2}$ құраушылар (категория атауы мен оған берілген түсініктеме), ал қалғандары – құрастырушылар, осыған байланысты (2.1.п. есепке ала отырып) қатер деңгейін $\boldsymbol{BC_3}$ компоненті арқылы беруге болдады.

Сұраныстарда берілетін барлық қаралып жатқан әрекеттер ($\boldsymbol{BC_1}$) қатер категориясында жинақталған, мысалы, BC_{11} сұраныс үлгісінде қаралған әрекет «Бизнестегі күтілмеген жағдай (БКЖ)» қатер категориясына кіреді, демек, берілген қатер категориясында сипаттаманы $\boldsymbol{BC_{1БКЖ}} = \{BC_{1БКЖ1}, BC_{1БКЖ2}, ..., BC_{1БКЖbc_1}\}$, мұндағы $BC_{1БКЖ1}$=«Ұрлық» (bc_1–БКЖ категориясы үшін қауіп-қатер идентификаторларының саны) түрінде елестетуге болады.

Талдау көрсеткендей жүйеде $\boldsymbol{BC_2}$ компонентін тікелей қолдану жоқ, бірақ онымен логикалық байланыс байқалады, сондықтан оның болуы жанама деп есептейміз. Осында және кортежде жанама сипаттамаларды белгілеу үшін * белгісі яғни $\boldsymbol{BC_2^*}$ қолданылады. Берілген анализден кейін ҚКМ-н есепке ала отырып, бұл әдістемеге 2.1.п. кортежді мына түрде елестете аламыз: $<\boldsymbol{BC_1}, \boldsymbol{BC_2^*}, \boldsymbol{BC_3}>$.

ҚБАҚ 8 - CRAMM (CCTA Risk Analysis and Management Method, өңдеуші – компьютерлер мен телекоммуникациялар бойынша Орталық агенттігі (CCTA – Central Computer and Telecommunications Agency), Великобритания**) әдісі** [62, 63]**.**

Қатерді анализдеу бірінші және екінші кезеңдерде өткізіледі де, онан соң оны бағалау жүзеге асырылады. Талдау кезінде қауіп-қатерді жүзеге асыру ықтималдылығы мен қауіп-қатердің пайда болу жиілігінің көзқарасы жағынан әрбір ресурс үшін коэффициенттерді қою ұсынылады, осыған орай 2.1.п. есепке ала отырып, мұнда $\boldsymbol{BC_5}$ және $\boldsymbol{BC_3}$ компоненттерін ерекше алуға болады.

CRAMM-де ҚКМ елестетуіне байланысты (COBRA әдістемесіне ұқсас) $\boldsymbol{BC_1}$, $\boldsymbol{BC_2^*}$ мәндерін анықтауға болады. $\boldsymbol{BC_1}$ компоненті әрекетпен кескінделгендіктен ақпараттық қауіпсіздік сипаттамасының бұзылуына алып

келген, мұны мына мысалда көрсетуге болады: «қауіп-қатер бағасы», дәлірек айтсақ, BC_{12}=«Рұқсат етілмеген мүмкіндік» BC_{21}=«Құпиялылықтың бұзылуына (ҚБ)» алып келуі мүмкін.

2.1.п. есепке ала отырып жүргізген талдаудан кейін берілген әдіске ҚКМ құрастырайық: <BC_1, BC_2^*, BC_3, BC_5, BC_6>.

ҚБАҚ 9 - RiskWatch (RiskWatch-АҚШ өндеуші компаниясы) **жүйесі** [62].

RiskWatch үшін 2.1. п. есепке ала отырып ҚКМ қатысты кортежді анықтайық. Осылай BC_1 компонентіне (берілген үлгідегі зақымдану категориясынан шыға отырып) мысалы, BC_{11}=«Қызмет көрсетуден бас тарту мен ірку», BC_{12}=«Ақпараттың ашылуы», BC_{13}=«Құрал-жарақтың жойылуы» т.б. мәндері сәйкес келеді. Бұл әрекеттер шабуыл жасалған ресурстардың ақпараттық қауіпсіздікгі белгілі бір сипаттамалардың бұзылуына алып келеді де, сәйкесінше BC_{23}=«ҚЖБ», BC_{21}=«ҚБұз», BC_{25}=«ТҚЖБ» мәндерімен байланысады. Талдау көрсеткендей жүйеде BC_2 компонентін тікелей қолдану жоқ, бірақ онымен логикалық байланыс байқалады, сондықтан оның болуы жанама деп есептейміз. Қатер талдауы 1-сатыны өту кезінде қолданылатын ТС арқылы инициализацияланатын мәліметтерді өңдеу кезінде жүргізіледі. *ALE* анықтау үшін BC_5 компоненті қолданылады, ал бір жылда күтілетін (BC_6) шығын түрінде түрлендіруге болатын зақымданулар қатер болып табылады. ҚКМ есепке ала отырып, бұл әдістеме үшін кортежді мына түрде елестетуге болады: <BC_1, BC_2^*, BC_5, BC_6>.

ҚБАҚ 10 - RA2 art of risk (RA Software Tool, AEXIS Security Consultants пен XiSEC Consultants Ltd.-Ұлыбритания өндеуші компаниясы) **аспабы** [8].

ҚКМ қатысты BC_1, BC_2 мәндерін анықтайық. Сұраныстарда берілетін (BC_1) барлық әрекеттер стандарт талаптары түрінде берілді, мысалы, «Үшінші біреулердің қол жеткізулерімен (ҮБҚЖ) байланысты қатерлерді анықтау үшін бағалау жүргізілді ме?», «Басқармамен ақпараттық қауіпсіздік саясаты мақұлданды ма?» т.б., бұл байланыста BC_1 компонентін BC_{1i}, $i = \overline{1, bc_1}$ (мұндағы bc_1 – қауіп-қатер идентификаторлар саны) түрінде кешенді беруге болады. Осылай, мысалы, берілген бағалауды орындамаған кезінде ҮБҚЖ туралы сұраныста ақпараттық қауіпсіздік сипаттама қорының бұзылуына алып келетін әрекеттер пайда болуы мүмкін, онда BC_1-ін $BC_{1\text{¾ª æ}} \in \{BC_{1\text{¾ª æi}}\} i = \overline{1, bc_1}$ жиынтығы түрінде елестетуге болады, мұндағы, мысалы, $BC_{1УБҚЖ1}$=«Ұрлық». BC_2 компонентіне қатысты айта кетеін жайт, қарастырылған әрекеттер (көрсетілген сұраныс үлгісінен шыға отырып) Ақпараттық қауіпсіздік белгілі бір сипаттамаларының бұзылуына алып келеді де, BC_{27}=«ҚТҚЖБ» мәнімен жанама байланысты болуы мүмкін. Талдау ПҚам-дағы BC_2^* сипаттамасы жанама түрде болып тұрғанын көрсетіп отыр. Әдістемеде BC_4 (қауіптілік деңгейі) мен BC_3 (қатер ықтималдығы) сипаттамалары бар, сондықтан қатер ұйым үшін (қатерлі жағдай басталған кезде) (BC_4) қауіптілік түрінде беріледі. ҚКМ-ін есепке ала отырып, бұл әдістеме үшін кортежді былай елестетуге болады: <BC_1, BC_2^*, BC_3, BC_4 >.

ҚБАҚ 11 - «АванГард» Ақпараттық қауіпсіздік басқару КСЖ-нің жүйесі (Кешенді сапшылар жүйесі «АванГард», өңдеуші – РҒА жүйелі талдау Институттың проблемасын ақпараттандыратын жүйелі талдау лабораториясы, Ресей) [64].

Айта кететін жайт, ҚКМ қатысты КСЖ-де, ақпараттық қауіпсіздіктің бұзылуына алып келетін (***BC₁***) әрекеті түрінде бейнелентін қатер оқиғасы қарастырылады, мысалы, BC_{11}=«хакер шабуылының себебінен веб-сервер қызметінің істен шығуы», BC_{12}=«Асыра қолданғандықтан криптосервердің құлдырауы», BC_{13}=«Тұтынушы құпия сөздерін басып алу» т.б. Әрекеттер сипаттамасында (қатер атауларында) көптеген өзіндік факторларының яғни өмір деңгейінің, халықтың білімділігінің, оның тілінің т.б. Ақпараттық қауіпсіздік қақтығыстарының пайда болу табиғатына әсер етуінің себебінен әртүрлі аудандар (мысалы, Қазақстанда) үшін барлық уақыт қолданыла бермейтін шетелдік компаниялар жинаған статистикалық мәліметтер қолданылады. Үлгіде қаралған (***BC₁***) әрекеттер ақпараттық қауіпсіздік сипаттама қорының бұзылу (***BC₂***) оқиғаларымен байланысты болуы мүмкін, мысалы, BC_{23}-ден BC_{11}=«ҚЖБ», BC_{27}-ден BC_{12}=«ҚТҚЖБ», ал BC_{13} BC_{21}-тен=«ҚБұз» т.б., сондықтан $\boldsymbol{BC_2^*}$ сипаттамасы жүйеде жанама түрде кездеседі. Ал қатерді талдау процесінде қолданылатын өзге компоненттерде (***BC₄***) қауіп дәрежесі мен (***BC₃***) қауіп оқиғасының ықтималдығы кездеседі. Сонымен бірге, ***BC₆*** арқылы берілетін шығын көрсеткіші де қолданылады. Қатер деңгейін объект, қосалқы жүйе (процесстер), жергілікті орта, аудан және жалпы алғанда модель бойынша анықтау қауіп-қатер (бар болған құрылымдарға құрылымдық иерархиялық модельдер көлеміне қатысы) маңыздылығының көрсеткіштерін есептеу жолымен жүргізіледі. Яғни объекттің ҚТП-лы онымен байланысты ҚТП-дың қауіп-қатер қосындысына тең болады, ал қосалқа жүйе (процесс) ҚТП-лы оған енген объекттер қосындысына тең болады. Есептеудің нәтижесі диаграмма түрінде ұсынылады. RiskWatch (3-саты) ұқсастығы бойынша, шығынды бағалау қатер бағасын және оның оқиға ықтималдығының жүзеге асырумен сәйкес келеді. Есепте ұйымның жалпы қатері ақша эквивалентінде беріледі. Ол қатердің барлық оқиғаларының жалпы шығыны түрінде берілетінін және жүйеде жанама кездесетін $\boldsymbol{BC_6^*}$ сипаттамасы түрінде де берілуі мүмкін екенін айта кетейік. ҚКМ-ін есепке ала отырып, талдауды жүргізгеннен кейін КСЖ үшін <$\boldsymbol{BC_1, BC_2^*, BC_3, BC_4, BC_6^*}$> болады.

ҚБАҚ 12 - Enterprise Risk Assessor (Risk Advisor, Methodware-Жаңа Зеландия өңдеуші компаниясы) **жүйесі** [55].

Берілген ПҚам үшін ҚКМ кезінде ***BC₁, BC₂, BC₃, BC₄*** және ***BC₆*** сипаттама қорының кескінін алуға болады. Enterprise Risk Assessor-да қатер түрінде ақпараттық қауіпсіздік бұзылуына алып келуі мүмкін әрекеттер қарастырылады, мысалы, BC_{11}=«Құжаттарды ұрлау» BC_{21}=«ҚБ» логикалық байланыста болуы мүмкін, сондықтан $\boldsymbol{BC_2^*}$ сипаттамасы ПҚам-да жанама кездеседі. Қатерді талдау барысында сипаттама қорын айқын түрде ***BC₃*** және жанама түрде $\boldsymbol{BC_6^*}$ қосымша идентификациялауға болады (<$\boldsymbol{BC_6^*}$ түрінде

елестетуге болатын consequence – салдар), ал оны бағалау кезінде – коэффициент мәні мен (***BC₄***) қауіп деңгейі орнатылады, сондықтан кортеж мынадай түрге ие болады: <***BC₁, BC₂****, ***BC₃, BC₄, BC₆****>.

ҚБАҚ 13 - vsRisk, Risk Assessment Tool (өңдеуші – компания Vigilant Software Ltd., Ұлыбритания) **жүйесі** [66].

Қатер талдауы кезеңінде бастапқы мәліметтер түрінде ***BC₁*** қызмет етеді де, мысалы, 1.10-суретіне сай ол BC_{23}=«ҚЖБ» мәніне алып келетін BC_{13}=«Қызмет көрсетуден бас тарту» мәнін қабылдауы мүмкін (1.11-суреті).

Жүйе қатердің барлық факторларын, сонымен бірге қауіп-қатерді, әлсіздікті, белсенділер мен бақылау механизмін қосқанда бағалау үшін құралдарды ұсынады да, тек сапалы шкалалармен ғана шектеліп, қатердің көлемін санды бағалау үшін құралдарға ие емес болып келеді. Айта кететін жайттардың бірі, бағалау үшін (***BC₃***) ықтималдылық маштабтары мен қарастырылып жатқан қауіп-қатерлердің әсер етуі беріледі, оларды ***BC₄**** деңгейі арқылы жанама елестете алуға болады. Жұмыстың жүруі барысында өнімнің мәліметтер қорына енгізілетін барлық өзгерістері егжей-тегжейлі түрде тексеру журналында белгіленеді.

ҚКМ есепке ала отырып, осы **ПҚам** үшін кортеж келесі түрде: <***BC₁, BC₂****, ***BC₃, BC₄****> болатынын айта кетейік**.**

ҚБАҚ 14 - OCTAVE (өңдеуші – институт Carnegie Mellon Software Engineering Institute пен Білім беру Орталығы, зерттеулер мен технологиялар (CERT), өнім тізімінде жүзеге асқан: OCTAVE әдісі, OCTAVE-S пен OCTAVE Allegro – сәйкесінше ірі, орташа және кіші ұйымдар үшін, АҚШ) **жүйесі** [56]**.**

Сипаттама қорына қатысты ҚКМ келтірейік, ПҚам-да ***BC₁, BC₂**** кездеседі. Қауіп-қатерді қаралған сценарий үлгісінде BC_{11}=«Медициналық жазбаларға рұқсат етілмеген қол жеткізу» сипаттамасы түрінде елестетуге болады, бұл логикалық түрде BC_{21}=«ҚБ» алып келеді. Қауіп «Қауіптілік» түрінде қаралады, мысалы, беделін жоғалту т.б., ***BC₄*** сипаттамасымен байланысты. Көрініп тұрғандай, кортеждің жалпы жазбасы OCTAVE үшін: <***BC₁, BC₂****, ***BC₄***>.

ҚБАҚ 15 - Callio Secura 17799 (өңдеуші – компания Callio Technologies, Канада) **аспабы** [67].

ҚКМ байланысты ***BC₁*** сипаттамасының (көрсетілген сұраныс үлгісінен шыға отырып) RA2 art of risk ұқсастығы бойынша, $BC_{1i},\ i=\overline{1,bc_1}$ кешенді түрде қарастыруға болады (bc_1 – қауіп-қатер идентификаторларының саны). Сонымен, мысалы, қауіпсіздік саясатына байланысты, ол жоқ болса, АҚ сипаттама қорының бұзылуына алып келетін іс-әрекеттер пайда болуы мүмкін. Мұндай жағдайда ***BC₁*** сипаттамасын $BC_{1^{2}\,\tilde{N}}\in\left\{BC_{1^{2}\,\tilde{N}\,i}\right\}\ i=\overline{1,bc_1}$ түрінде елестетуге болады, мұндағы, мысалы, $BC_{1^{2}\,\tilde{N}\,1}$=«Құпиялы ақпараттың жоғалуы». Өз кезегінде бұл әрекеттің кешені АҚ-ның сипаттама қорының бұзылуына алып келуі мүмкін және BC_{27}=«ҚЖТҚБ» мәнімен де байланысуы мүмкін. Сонымен бірге, ***BC₃*** (қауіп-қатер ықтималдығы) және ***BC₆*** (белсенділердің құндылығы – ұйым үшін

шығын, логикалық түрде шығын немесе жоғалту түрінде анықталады) бар болуын атап өтуге болады. Міне осылай, кортежді былай суреттейміз: <BC_1, BC_2, BC_3, BC_6>.

ҚБАҚ 16 - Гриф 2006 (Digital Security-Ресей өңдеуші компаниясы) **жүйесі** [62].

ҚКМ позициясы жағынан Гриф 2006-ны қарастырайық. Осылай, (сұраныстың көрсетілген үлгісінен шыға отырып) BC_1 сипаттамасына BC_{11}=«Ақпараттың ашылуы» мәні сәйкес келеді. Бұл әрекет құпиялылықтың бұзылуына алып келеді де, BC_{21}=«ҚБ» мәнімен байланысады. Қауіптің бағалануы компоненттердің көмегімен жүзеге асады: BC_3 – қауіп-қатерді жүзеге асыру ықтималдығы, BC_6^* – оны жүзеге асырудағы шығын және BC_4^* – әлсіздігі бойынша қауіп-қатер деңгейі. Көрсетілген ПҚ үшін кортеж құрастырайық: <BC_1, BC_2, BC_3, BC_4^*, BC_6^*>.

ҚБАҚ 17 - @RISK (өңдеуші – компания Palisade, АҚШ) **жүйесі** [68].

Осы жүйеде қолданылатын қауіптің сипаттама қорына байланысты BC_1 мен BC_2 бар екенін айта кетейік. Логикалық түрде анықтауға болатын, (BC_1) әрекеті алып келетін АҚ сипаттамасының бұзылу оқиғасы түрінде BC_2^* сипаттамасы жанама түрде берілген, мысалы, BC_{13} =«Алаяқтық» BC_{27} =«ҚЖТҚБ» алып келуі мүмкін. Қатерді бағалау кезінде (BC_3) ықтималдығы қойылады да, әсер етуі есептеледі, мұны BC_6^* – шығын түрінде елестетуге болады. Көрініп тұрғандай бұл кортеж мынадай болады: <BC_1, BC_2^*, BC_3, BC_6^*>.

ҚБАҚ 18 - RiskPAC (өңдеуші – компания CSCI, Нидерландия) **жүйесі**. ҚКМ байланысты ПҚ мәліметтерін қарастырайық. Сонымен, BC_1 сипаттамасына сәйкес келеді (сұраныс үлгісінен көрініп тұрғандай), мысалы, BC_{11} мәні. Бұл әрекет шабуыл жасалған ресурстардың АҚ сипаттамасының белгілі бір бұзылуларына алып келеді де, BC_{25}=«ҚЖТБ» мәнімен байланысты болып келуі мүмкін. Қатерді бағалау кезінде, (BC_6) жоғалту мен (BC_4) қауіптілік деңгейін интерпретациялауға болатын, (BC_3) қауіп-қатер ықтималдығы, әсер ету анықталады. Келтірілген анализдің көрсетуі бойынша кортеж бұл жүйе үшін мына түрге ие: <BC_1, BC_2^*, BC_3, BC_4, BC_6>.

ҚБАҚ 19 - Microsoft Security Assessment Tool (MSAT, өңдеуші – компания Microsoft, США) **жүйесі** [47].

ҚКМ байланысты ПҚ-да BC_1 және BC_2 суреттелген. Қаралған сұраныс «Оқиғаның кірісіне әсер етеді ма…» үлгісіндегі оқиғаны BC_{11}=«Түйіннің әрекетсізденуі», BC_{12}=«Құрылғының істен шығуы» және BC_{13}=«Үстемелердің шалыс соғылуы» сипаттама түрінде елестетуге болады, бұл BC_{23}=«ҚЖБ» алып келуі мүмкін. Бағалау кезінде қатер қауіптілік түрінде қарастырылады (BC_4). Айта кететін жайт, MSAT үшін кортеж мынадай: < BC_1, BC_2^*, BC_4>.

ҚБАҚ 20 - Бейестік желілер негізіндегі әдіс (БЖӘ) [69].

ҚКМ қатысты БЖӘ үшін 2.1. п. есепке ала отырып кортежді анықтап алайық. Мысалда көрініп тұрғандай BC_1 компоненті BC_{11} =«Хакерлік шабуыл»

сәйкестене алады, бұл әрекет АҚ сипаттама қорының бұзылуына алып келеді де, BC_{27} =«ҚҚЖТБ» (Құпиялылық, Қол жетімділік, Тұтастық, Бұзылуы) мәнімен байланысты болуы мүмкін. Сонымен бірге, қатерді бағалау үшін бағалау компоненттері қолданылады: $\boldsymbol{BC_3}$ (абсолютті ықтималдылық пен оқиға нәтижесінің ықтималдығы), $\boldsymbol{BC_6}$ (зақымдану көлемі), $\boldsymbol{BC_4}$ (шығын).

Айта кететін жайттардың бірі, $\boldsymbol{BC_4^*}$ сипаттамасы тікелей жүйеде қолданылмайды, дегенмен онда логикалық байланыс бақыланып отырады (жанама болып табылады). ҚКМ ескере отырып, анализді жүргізіп болған соң, берілген әдіс үшін кортеж құрамыз: $<\boldsymbol{BC_1, BC_2, BC_3, BC_4^*, BC_6}>$.

ҚБАҚ 21 - VAR (Value at Risk) **әдісі** [68].

ҚКМ қатысты VAR үшін мынадай сипаттама қор мәндерін анықтап алуға болады: $\boldsymbol{BC_1}$ әрекет, АҚ сипаттамасының бұзылуына алып келуі мүмкін, бұл сұрақ үлгісінен көрініп тұр, яғни BC_{11}=«АҚ ережелерінің бұзылуы» BC_{27}=«ҚЖТҚБ» алып келуі мүмкін. Сонымен бірге қатерді бағалау барысында $\boldsymbol{BC_3}$, $\boldsymbol{BC_4}$ **және** $\boldsymbol{BC_6}$ сипаттама қорларын қолданады. ҚКМ есепке ала отырып, берілген әдіс үшін кортеж мына түрге: $<\boldsymbol{BC_1, BC_2^*, BC_3, BC_4, BC_6}>$.

ҚБАҚ 22 - TRA әдістемесі (Threat and Risk Assessment, өңдеуші – компания Government (Communications Security Establishment), Канада) [52].

ҚКМ-ін есепке ала отырып, айта кететін жайт, TRA-да $\boldsymbol{BC_1}$ сипаттамасы қауіп-қатер әрекетімен беріледі, мысалы, BC_{11}=«Тыңшылық» (5-кестеде көрініп тұрғандай), бұл өз кезегінде BC_{21} =«ҚБ» алып келеді. Қатерді бағалау $\boldsymbol{BC_3}$ мен $\boldsymbol{BC_4^*}$ сипаттамаларына негізделген. Талдаудың көрсетуі бойынша берілген әдістеме үшін кортеж келесі түрде: $<\boldsymbol{BC_1, BC_2, BC_3, BC_4^*}>$.

ҚБАҚ 23 - FRAP (Facilitated Risk Analysis Process, өңдеуші – компания Peltier and Associates, АҚШ) **әдістемесі** [21]**.**

ҚКМ қатысты берілген әдістемені қарастырайық. Демек, $\boldsymbol{BC_1}$ сипаттамасына қауіп-қатер жиынтығы сәйкес келеді (мысалы, эксперттер құраған), бұл өз кезегінде ақпараттық қауіпсіздікіпсіздіктің сипаттама қорының бұзылуына алып келуі мүмкін. Әдістемеде $\boldsymbol{BC_2^*}$ сипаттамасының тікелей қолданылуы жоқ, бірақ олардың арасында логикалық байланыс бақыланады, сондықтан олардың бар болуын жанама деп есептейміз. Қатерді бағалау қауіп-қатер ықтималдығына ($\boldsymbol{BC_3}$) және шығынына ($\boldsymbol{BC_6}$) негізделген. Анализ көрсетуі бойынша осы әдістеме үшін кортеж мынадай түрге ие: $<\boldsymbol{BC_1, BC_2^*, BC_3, BC_6}>$.

ҚБАҚ 24 - Risk Matrix әдістемесі (өңдеуші компания Mitre Corporation, АҚШ) [73].

ҚКМ қатысты қолдағы сипаттамаларды қатер матрицасының үлгісінде қарастырайық (1.18-суретінде). Мұнда әрекеттерді BC_{27}=«ҚТҚЖБ» логикалық байланысқа ие BC_{11}=«ПҚ жаңартылмайды» параметрі арқылы суреттеуге болады. Бағалау кезінде $\boldsymbol{BC_5}$, $\boldsymbol{BC_3}$ қолданылады, ал $\boldsymbol{BC_4^*}$ жанама қолданылады

(әсер ету түрінде берілген). Risk Matrix үшін кортеждің жалпы жазбасы мынадай түрге ие: <BC_1, BC_2^*, BC_3, BC_4^*, BC_5>.

ҚБАҚ 25 - Mehari әдіснамасы (өңдеуші Clusif, Франция) [74].

Әрекет сұранысының қаралған «Қуат беруді реттейтін жүйе бар ма …» үлгісінде, мысалы, BC_{11}=«Құрал-жабдықтың істен шығуы», BC_{12}=«Үстеменің жаңылуы» т.б. параметр түрінде елестетуге болады, бұлар BC_{23}=«ҚЖБ» алып келуі мүмкін. (BC_4) Қауіптілік деңгейімен түсіндіруге болатын қатерді әсер ету түрінде қарастырылады. Айта кететін жайт, Mehari үшін кортеж мынадай: < BC_1^*, BC_2^*, BC_4^*>.

ҚБАҚ 26 - MAGERIT әдістемесі (Methodology for Information Systems Risk Analysis and Management, өңдеуші Ministerio De Administraciones Públicas, Испания) [75].

ҚКМ қатысты қарастырылған (1.24-кестеде қара) үлгіде қауіп-қатерді BC_1 сипаттамасы түрінде түсіндіруге болады, мысалы, BC_{11}=«Рұқсат етілмеген мүмкіндік». Бұл әрекет BC_{21}=«ҚБ» оқиғасына алып келуі мүмкін. Сонымен бірге бағалау барысында BC_5, BC_6, BC_4 мен BC_3 сипаттамалары қолданылады. Сондықтан, MAGERIT үшін кортеждің жалпы жазбасы: <BC_1, BC_2^*, BC_3, BC_4, BC_5, BC_6>.

ҚБАҚ 27 - Information Security RA әдістемесі (Risk Assessment, өңдеуші Centers for Medicare & Medicaid Services (CMS), АҚШ) [76].

ҚКМ қатысты берілген әдістемені қарастырамыз. Демек, BC_1 сипаттамасына 2-сатыда анықталатын барлық қауіп-қатерлер сәйкес келеді. Олар АҚ сипаттама қорының бұзылуына алып келуі мүмкін, сондықтан BC_2^* мәндерімен байланысуы мүмкін. Оның әдістемеде тікелей қолданылуы жоқ екендігін талдау көрсетті, бірақ онымен логикалық байланыс байқалады, демек жанама кездеседі. Қатерді бағалау кезінде (BC_3) қауіп-қатер мен әсер ету ықтималдығы анықталады, мұны BC_4^* сипаттамасымен бейнелеуге болады. Зерттеу көрсеткендей бұл жүйе үшін кортеж мына түрге ие: <BC_1, BC_2^*, BC_3, BC_4^*>.

Міне осылай, 2.1. п. ұсынылған амалды есепке ала отырып, жұмыста ҚБАҚ кең спекторын зерттеу сәйке келетін ПҚам түрінде жүргізілді және сәйкес келетін бағалау құралдарын салыстырмалы талдауын жүзеге асыруға болатын, АҚор мәселелерінің белгілі бір класын шешу үшін тиімдірегін таңдап алуға болатын сипаттама қорының жиынтығы (2.2-кестеге қара) анықталды.

Көрініп тұрғандай тек екіжүйе ИББС-2.2-2009 пен MAGERIT ғана қатер параметрлерінің толық жиынтығын бейнелейді, олар қатерді бағалауды жүзеге асыру кезінде маманның мүмкіндігін кеңейтеді.

Кесте 2.2 - ҚБАҚ зерттеуінің нәтижесі

ВС ҚБАҚ	$ВС_1$	$ВС_2$	$ВС_3$	$ВС_4$	$ВС_5$	$ВС_6$
1	2	3	4	5	6	7
1	+	+*	+	-	-	-
2	+	+*	+	-	+	+
3	+	+*	-	-	+	+
4	+	+*	+	+	-	-
5	+	+*	+	+	-	+*
6	+	+*	+	+	-	+*
7	+	+*	+	+*	-	-
8	+	+*	-	+	-	-
9	+	+	+	-	-	+
10	+	+	+	+*	-	+*
11	+	+*	+	-	-	+*
12	+	+*	+	+	-	+
13	+	+*	-	+	-	-
14	+	+	+	+*	-	+
15	+	+*	+	+	-	-
16	+	+*	+	+	-	+
17	+	+	+	+*	-	-
18	+	+*	+	-	-	+
19	+	+	-	-	-	-
20	+	+*	+	+	+	+
21	+	+*	+	+	-	-
22	+	+*	+	+*	+	-
23	+	+*	+	+*	-	-
24	+*	+*	-	+*	-	-
25	+*	+*	+	+*	-	-
26	+	+*	+	+	+	+
27	+	+*	+	+*	-	-

2.3 Ақпараттық қауіпсіздікті басқару жүйесі үшін қатерді бағалаудың FirstM әдісі

Ақпараттық қауіпсіздік қамтамасыздандыру үшін ISO/IEC 27001 стандартының ұсынысына сәйкес кәсіпорында әртүрлі меншіктік түрінде ақпараттық қауіпсіздік менеджменті жүйесін енгізу қажет [8]. Мұндай стандарттың негізі ақпараттық қауіпсіздік қатерінің менеджменті болып табылады. Бұл жерде ақпараттық қауіпсіздік қатерін өңдеу мен бағалау, анализдеу түсініледі. Жұмыста қатер сипаттама қорының кортежді моделі (2.1. п.) ұсынылды, сонымен бірге болашақта сәйкес келетін құралдарды салыстыру мен анализдеу үшін қолдануға болатын ҚБАҚ-ң (2.2 п.) сипаттама қорының анықталуымен кең спектрі зерттелді. Мұндай зерттеу қатерді бағалау мен анализдеу үшін көбіне ақпараттық қауіпсіздік қауіп-қатер мен қақтығыстар туралы статистикалық мәліметтер қолданылатынын көрсетті. Көптеген елдерде (соның ішінде Қазақстанда) мұндай статистика мемлекеттік деңгейде жүргізілмейді, бұл өз кезегінде ұлттық қолдану үшін бар болған құралдардың

мүмкіндіктерін шектейді. Сонымен бірге зерттеліп жатқан аспап сарапшыға белгілі бір (қолданылып жатқан параметрлер жиынтығына) шектеулер қоятынын және көлемнің кеңірек спектрін бағалау үшін қолдану мүмкіндігін бермейтінін айтып кету керек.

Осыған байланысты бағалаудың икемдірек құралдарын жасауға мүмкіндік беретін, сипаттама қорының кең спектрін қолдануға мүмкіндік беретін, сонымен бірге қатерерді уақыт мерзімін, саланы, кәсіпорынның экономикалық және басқарушылық ерекшеліктеріне т.б. есепке ала отырып, анықталмаған, төмен нысандандырылған ортадағы статистикалық мәліметтер негізінде де, сарапшылық бағалау негізінде де анықтауға мүмкіндік беретін қатерді бағалау мен анализдеу әдістерін өңдеу бұл – мақсат болып табылады. Сонымен бірге өңделіп жатқан әдістер параметрлер сипаттайтын тек қана сандық түрде емес, сонымен бірге сапалық түрде де сипаттайтын күрделі жүйелерді сипаттау үшін жиі қолданылатын ЛА қолдана отырып сандық түрде де, ауызша түрде де нәтижелерді қамтып көрсетуге мүмкіндік береді. Сонымен бірге ЛА сапалық мәндерге белгілі бір эквивалент санына сәйкестендіріп қоюға мүмкіндік береді [77]. Қойылған мәселені шешу үшін сарапшылар талқылауына негізделген амалды қолдану ұсынылады. Осылай бола тұра бірінші жағдайды яғни бағаланып жатқан параметрлер мәндеріне қатысты сарапшы нақты (бинарлық) артықшылығы бар екенін есепке аламыз, сонымен бірге екінші жағдайды да сенімсіз аймағын яғни сарапшы өз артықшылығының бір мағыналылығында сенімсіз болуын есепке аламыз. Осыған сәйкес бағалаудың екі әдісі – детерминдендірілген (FirstM) [78] және нақты емес төмен нысандандырылған орта (SecondM) [79].

FirstM әдісі

1-кезең - Жиынтықты анықтау. Бұл кезеңде барлық қолданылып жатқан параметрлердің жиынтық қоры анықталады да, қатерді бағалау мен анализдеу барысында іске қосылады. Жиынтықты анықтау үшін қатер сиаттама қорының кортежді моделін (2.1 п.) негіз түрінде қолданамыз: $\boldsymbol{BC_2} = \bigcup_{i=1}^{7} BC_{2i}$ – АҚ бұзылу оқиғасына (мысалы, $\boldsymbol{BC_2}$ BC_{27}=«ҚТҚЖБ» мәнімен беріледі), $\boldsymbol{BC_2}$ -не алып келетін (мысалы, bc_1=5 үшін сарапшылар)

$\boldsymbol{BC_1} = \bigcup_{i=1}^{5} BC_{1i} = \{BC_{11}, BC_{12}, BC_{13}, BC_{14}, BC_{15}\}$={«Вирустардан зақымдану», «Программалау қателіктері», «Операциялық жүйе жұмысының бұзылуы», «Қауіпсіздік жүйесі тұтастығының бұзылуы», «Қызмет көрсетуден бас тарту»} идентификациялауы мүмкін) $\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i}$ – әрекет;

Қатерді бағалаудың жалпы нәтижесін елестету үшін [80] <*LR*, $\underset{\sim}{T}_{LR}$, X_{LR}> кортежімен анықталатын «ҚАТЕР ДЕҢГЕЙІ» (***LR***) ЛА қолданайық, мұндағы

терм-жиынтық қоры m термдермен беріледі: $\underset{\sim}{\boldsymbol{T}}_{LR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{LR_j}$ (мысалы, m=5 үшін – $\bigcup_{j=1}^{5} \underset{\sim}{T}_{LR_j}$ = {«АҚ бұзылу қатерінің деңгейі өте төмен» (ҚТ), «АҚ бұзылу қатерінің деңгейі төмен» (ТҚ), «АҚ бұзылу қатерінің деңгейі орташа» (ҚО), «АҚ бұзылу қатерінің деңгейі жоғары» (ҚЖ), «АҚ бұзылу қатерінің деңгейі өте жоғары» (ЖҚ)}, бұлар $X_{LR} \in \{0, max_{LR}\}$ әмбебап жиынтықта көрінуі мүмкін). Термдердің $\underset{\sim}{T}_{LR_1}, \ldots, \underset{\sim}{T}_{LR_j}, \ldots, \underset{\sim}{T}_{LR_m}$ әр біріне өз арақашықтық мәні $[lr_{min}; lr_1[, \ldots, [lr_j; lr_{j+1}[, \ldots, [lr_m; lr_{max}]$ беріледі (мысалы, m=5 кезінде $\underset{\sim}{T}_{LR_1}$, $\underset{\sim}{T}_{LR_2}$, $\underset{\sim}{T}_{LR_3}$, $\underset{\sim}{T}_{LR_4}$, $\underset{\sim}{T}_{LR_5}$ үшін Харрингтон шкалаларын қолдана отырып арақашықты анықтайық [26], кейін оның дәйеклелген маңыздылықтарын үлкейту арқылы екі тәртіпте яғни $[lr_{min}; lr_1[$, $[lr_2; lr_3[$, $[lr_4; lr_5[$, $[lr_6; lr_7[$, $[lr_8; lr_{max}]$ өзгертеміз, бұлар мына маңыздылықтарға сәйкес келетін болады - [0; 20[, [20; 40[, [40; 60[, [60; 80[, [80; 100]). Әрі қарай сарапшының бағалау кезінде көлем спектрінің кеңірегін қолдануына мүмкіндік жасау үшін жоғарыда айтылған қатер сипаттама қорының моделін қолданамыз да, мынау сияқты көптеген сипаттамалар береміз: $\boldsymbol{EC}_{Fh} \in \{EC_i\} = \{\boldsymbol{BC_3}, \boldsymbol{BC_4}, \boldsymbol{BC_5}, \boldsymbol{BC_6}\}$ ($i = \overline{1,g}$), мұндағы Fh – он алтылық код, жиынтықта сипаттаманың реттік номерін көрсетін оның бинарлық мәні мынадай түрде: $\boldsymbol{BC_3}$ 2^3, $\boldsymbol{BC_4}$ в 2^2, $\boldsymbol{BC_5}$ – 2^1, $\boldsymbol{BC_6}$ – 2^0 разрядында орналасады (мысалы, егер сарапшылар $\boldsymbol{BC_3}$, $\boldsymbol{BC_4}$ мен $\boldsymbol{BC_6}$ қолданғысы келсе, онда g=3 ($i = \overline{1,3}$), ал $\boldsymbol{EC}_{Dh} \in \{EC_i\} = \{\boldsymbol{EC_1}, \boldsymbol{EC_2}, \boldsymbol{EC_3}\} = \{\boldsymbol{BC_3}, \boldsymbol{BC_4}, \boldsymbol{BC_6}\}$).

[80] $< C_{EC_i}, \underset{\sim}{T}_{C_{EC_i}}, X_{EC_i} >$ кортежімен анықталатын ЛА «ҚАТЕР ДЕҢГЕЙІН EC_i» (C_{EC_i}) енгізейік, мұндағы терм-жиынтық қоры m термдерімен $\underset{\sim}{\boldsymbol{T}}_{C_{EC_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{C_{EC_i j}}$ беріледі (мысалы, m=5 кезінде – $\bigcup_{j=1}^{5} \underset{\sim}{T}_{C_{EC_i j}}$ = {«Өте төмен» (ӨТ), «төмен» (Т), «орташа» (О), «жоғары» (Ж), «өте жоғары» (ӨЖ)}, олар лингвистикалық түрде деңгей сипаттамасын сипаттайды да, әмбебап жиынтыққа суреттелуі мүмкін $X_{EC_i} \in \{0, \max_{C_{EC_i}}\}$). $\underset{\sim}{T}_{C_{EC_i 1}}, \ldots, \underset{\sim}{T}_{C_{EC_i j}}, \ldots, \underset{\sim}{T}_{C_{EC_i m}}$ үшін сәйкесінше өз арақашықтық мәнінің әр бір EC_i – $[c_{EC_i \min}; c_{EC_i 1}[$, …, $[c_{EC_i j}; c_{EC_i j+1}[, \ldots, [c_{EC_i m}; c_{EC_i \max}]$ (мысалы, m=5 кезінде EC_3={$\boldsymbol{BC_6}$} сипаттама қорындағы $\underset{\sim}{T}_{C_{EC_3 1}}$, $\underset{\sim}{T}_{C_{EC_3 2}}$, $\underset{\sim}{T}_{C_{EC_3 3}}$, $\underset{\sim}{T}_{C_{EC_3 4}}$, $\underset{\sim}{T}_{C_{EC_3 5}}$ термдері үшін маңыздылықтарының арақашыққа бөлінуін - $[c_{EC_3 \min}; c_{EC_3 1}[$, $[c_{EC_3 2}; c_{EC_3 3}[$, $[c_{EC_3 4}; c_{EC_3 5}[$, $[c_{EC_3 6}; c_{EC_3 7}[$, $[c_{EC_3 8}; c_{EC_3 \max}]$ жүзеге асырайық, оған мына мәндер сәйкес келеді [0; 0,1[, [0,1; 0,2[, [0,2;

0,3[, [0,3; 0,4[, [0,4; 0,5]) беріледі. Мүмкін болған арақашықтық мәні арқылы сипаттама қорының бейнеленуін ыңғайластыру үшін 2.3-кестесін қолданамыз. EC_i маңыздылығын бағалау $\boldsymbol{LS} \in \{LS_i\}\,(i=\overline{1,g})$, жиынтық параметрлері арқылы жүзеге асырылады, ал бағалау кезектегі компоненті маңыздылықтарының баға $\boldsymbol{ec} \in \{ec_i\}\,(i=\overline{1,g})$ жиынтығы көмегімен жүзеге асырылады.

Кесте 2.3 - Сипаттама қор маңыздылықтарының бейнеленуі

EC_i	$\underset{\sim}{T}_{C_{EC_i1}} - \underset{\sim}{T}_{C_{EC_im}}$ үшін C_{EC_i} мәндерінің арақашықтығы				
	$\underset{\sim}{T}_{C_{EC_i1}}$	…	$\underset{\sim}{T}_{C_{EC_ij}}$	…	$\underset{\sim}{T}_{C_{EC_im}}$
EC_1	$[c_{EC_1\min}; c_{EC_11}[$	…	$[c_{EC_1j}; c_{EC_1j+1}[$	…	$[c_{EC_1m}; c_{EC_1\max}]$
…	…	…	…	…	…
EC_i	$[c_{EC_i\min}; c_{EC_i1}[$	…	$[c_{EC_ij}; c_{EC_ij+1}[$	…	$[c_{EC_im};]$
…	…	…	…	…	…
EC_g	$[c_{EC_g\min}; c_{EC_g1}[$	…	$[c_{EC_gj}; c_{EC_gj+1}[$	…	$[c_{EC_gm}; c_{EC_g\max}]$

2-кезең - Сипаттама қорының суреттелуі. Бұл кезеңде қолданылып жатқан сипаттама қоры жинағының суреттелуі жүргізіледі, бұл сарапшы-аналитиктердің пікірінше бір жағынан АҚ қатерінің бағалауына әсер етсе, екінші жағынан оның әр түрлі табиғи жақтарын бағалайды дейді, мысалы, ұйымның есепке алушы ерекшеліктерін (банк, архив, күш беретін тізімдеме, зауыт т.б.). Ол үшін сарапшы он алтылық кодты анықтауы қажет, бұл бойынша $\{EC_i\}$-тен сәйкес келетін компонент маңыздылығы таңдалады, мысалы, *Dh* кезінде – g=3 болады, ал $\boldsymbol{EC}_{Dh} \in \{EC_i\} = \{\boldsymbol{EC_1, EC_2, EC_3}\} = \{\boldsymbol{BC_3, BC_4, BC_6}\}$ $(i=\overline{1,3})$ болады немесе *Fh* коды кезінде – g=4 болады, ал $\boldsymbol{EC}_{Fh} \in \{EC_i\} = \{\boldsymbol{EC_1, EC_2, EC_3, EC_4}\} = \{\boldsymbol{BC_3, BC_4, BC_5, BC_6}\}$ $(i=\overline{1,4})$ болады.

3-кезең - Сипаттама қорындағы маңыздылық деңгейдің бағалануы.

Бұл кезеңде EC_i – әрбір компонентіне оның LS_i – маңыздылық деңгейі сәйкесінше қойылады. Айта кететін жайт, егер барлығы үшін *LS* болса

$$LS_i \geq LS_{i+1}, \tag{2.1}$$

онда *i*-лі компонент маңыздылығы Фишберн ережесі бойынша анықталады [27]:

$$LS_i = \frac{2(g-i+1)}{(g-1)g} \tag{2.2}$$

Осы ережеге байланысты сарапшыда (шарттан басқа (2.1)) компоненттің мағыналылығы туралы ақпарат жоқ, сонда (2.2) зерттеу объектісі туралы қолда бар ақпараттық белгісіздік энтропиясының максимумын суреттейді. Егер

барлық компоненттер теңдеу маңыздылыққа ие (теңдей ұнамды яғни $LS_i = LS_{i+1}$ немесе жүйеде ұнайтыны жоқ) болса, онда:

$$LS_i = 1/g\ . \qquad (2.3)$$

4-кезең - Қатер деңгей маңыздылығының эталонын анықтау.

Бұл кезеңде сарапшылар тарапынан *LR* үшін маңыздылық эталондары анықталады яғни ЛА терм-жиынтық қорында термдер саны беріледі және оларға сай [lr_{min}; lr_{max}] диапазонында жатқан өздерінің арақашықтық мәні беріледі (1-кезеңдегі үлгіні қара).

5-кезең - Сипаттама қор маңыздылығының эталонын анықтау. Мұнда сарапшылар тарапынан C_{EC_i} үшін этолонды маңыздылықты анықтау жүргізіледі яғни ЛА терм-жиынтығында термдер саны беріледі (2.3-кезеңіндегі үлгі мен 2.4-кестесін қара).

Кесте 2.4 - Қор компонент маңыздылығының эталонын анықтау үлгісі

EC_i	$\underset{\sim}{T}_{C_{EC_i1}} - \underset{\sim}{T}_{C_{EC_i5}}$ үшін C_{EC_i} маңыздылықтарының арақашықтығы				
	$\underset{\sim}{T}_{C_{EC_i1}}$	$\underset{\sim}{T}_{C_{EC_i2}}$	$\underset{\sim}{T}_{C_{EC_i3}}$	$\underset{\sim}{T}_{C_{EC_i4}}$	$\underset{\sim}{T}_{C_{EC_i5}}$
EC_1=**BC_3**	$\underset{\sim}{T}_{C_{BC_31}} \in$ [0; 20[	[20; 40[	[40; 60[	[60; 80[	$\underset{\sim}{T}_{C_{BC_35}} \in$ [80; 100]
EC_2=**BC_4**	$\underset{\sim}{T}_{C_{BC_41}} \in$ [0; 2[	[2; 4[	[4; 6[	[6; 8[	$\underset{\sim}{T}_{C_{BC_45}} \in$ [8; 10]
EC_3=**BC_5**	$\underset{\sim}{T}_{C_{BC_51}} \in$ [0;0,2[	[0,2; 0,4[	[0,4; 0,6[	[0,6; 0,8[	$\underset{\sim}{T}_{C_{BC_55}} \in$ [0,8; 1]
EC_4=**BC_6**	$\underset{\sim}{T}_{C_{BC_61}} \in$ [0;0,1[	[0,1; 0,2[	[0,2; 0,3[	[0,3; 0,4[	$\underset{\sim}{T}_{C_{BC_65}} \in$ [0,4; 0,5]

6-кезең - Кезектегі сипаттама маңыздылықтарының бағасы.

Бұл кезеңде әрбір $\{EC_i\}$=**{BC_3, BC_4, BC_5, BC_6}** ($i = \overline{1,g}$) сипаттама қоры бойынша сәйкес келетін пән аралық саладағы сарапшылар ($bc_1 = \overline{1,n}$) кезінде барлық ***BC_1*** үшін ***ec*** анықтайды яғни $\{ec_i^{BC_{1bc_1}}\}$=$\{ec_{BC_3}^{BC_{1bc_1}}, ec_{BC_4}^{BC_{1bc_1}}, ec_{BC_5}^{BC_{1bc_1}}, ec_{BC_6}^{BC_{1bc_1}}\}$. Маңыздылықтар сарапшылардың, статистикалық ақпараттардың т.б. мәліметтерінің ұнауына негізделіп қойылады. 2.5-кестесінде 1-кезеңде g=4 кезінде, ал $\boldsymbol{EC}_{Fh} \in \{EC_i\}$=**{$BC_3$, BC_4, BC_5, BC_6}** ($i = \overline{1,4}$) берілген, $\boldsymbol{BC_1} = \bigcup_{i=1}^{5} BC_{1i}$ үшін кезектегі маңыздылықтарды анықтау үлгісі берілген.

Кесте 2.5 - 1-үлгі – кезектегі сипаттама қоры маңыздылығының анықталуы

EC_i	$ec_i^{BC_{11}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{12}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{13}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{14}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{15}}$	$\underset{\sim}{T}_{C_{EC_i}}$
BC3,(*i*=1)	72	В	58	С	64	С	70	Ж	66	С
BC4,(*i*=2)	5,4	С	6	С	2,2	ОН	9	ӨЖ	5,5	С
BC5,(*i*=3)	0,72	В	0,58	С	0,64	С	0,7	Ж	0,66	С
BC6,(*i*=4)	0,23	С	0,33	С	0,12	Н	0,4	Ж	0,24	Н

7-кезең - Кезектегі маңыздылықтардың классификациясы.

Бұл кезеңді өту кезінде берілген диапазонға $ec_i^{BC_{1bc_1}}$ тиістілігі анықталады да, бұл бойынша бағалау параметрлеріне қатысты сарапшының артықшылығын көрсететін λ бинарлы маңыздылық қалыптасады:

$$\lambda_{ij}^{(BC_{1bc_1})} = \begin{cases} 1, \textit{егер } ec_i^{BC_{1bc_1}} \in [\, c_{EC_i(j-1)}; c_{EC_i j}[\\ 0, \textit{егер } ec_i^{BC_{1bc_1}} \notin [\, c_{EC_i(j-1)}; c_{EC_i j}[\end{cases}, \qquad (2.4)$$

ал нәтижесі ыңғайлы болу үшін 2.6-кестесіне енгізілді.

Кесте 2.6 - Кезектегі сипаттама қорының маңыздылық классификациясы

EC_i	$\underset{\sim}{T}_{C_{EC_i j}}$ $(i=\overline{1,g},\ j=\overline{1,m})$ үшін $\lambda_{ij}^{(BC_{1bc_1})}$				
	$\underset{\sim}{T}_{C_{EC_i 1}}$	…	$\underset{\sim}{T}_{C_{EC_i j}}$	…	$\underset{\sim}{T}_{C_{EC_i m}}$
EC_1	λ_{11}	…	λ_{1j}	…	λ_{1m}
…	…	…	…	…	…
EC_i	λ_{i1}	…	λ_{ij}	…	λ_{im}
…	…	…	…	…	…
EC_g	λ_{g1}	…	λ_{gj}	…	λ_{gm}

BC1 барлығы үшін ұқсас қайта жаңғырулар жүргізіледі, мысалы, 1-кезеңде анықталғандарға барлық анықталған маңыздылықтар $\lambda_{ij}^{(BC_{11})}$, $\lambda_{ij}^{(BC_{12})} \ldots \lambda_{ij}^{(BC_{15})}$ 2.7-кестесіне енгізейік.

8-кезең - Қатер деңгейін бағалау. Бұл кезеңде $lr^{(BC_{1bc_1})}$ формуласы бойынша АҚ бұзылу қатерінің көрсеткіш деңгейін есептеу жүзеге асырылады:

$$lr^{(BC_{1bc_1})} = \sum_{j=1}^{m} \left(lr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(BC_{1bc_1})} \right), \qquad (2.5)$$

мұндағы lr_j=90-20(j-1) $\lambda_{ij}^{(BC_{1bc_1})}$ (2.4) формуласы бойынша әрбір BC_{1bc_1} $(bc_1=\overline{1,n})$ анықталса, ал LS_i $(i=\overline{1,g})$ – (2.2) формуласы бойынша немесе (2.3) бойынша $(j=\overline{1,m})$ анықталады.

Кесте 2.7 - 1-Үлгі – кезекті сипаттама маңыздылықтарының классификациясы

EC_i	$BC_1 \in \{BC_{1bc_1}\}$ $(bc_1 = \overline{1,5})$ үшін λ маңыздылығы																									
	$\lambda_{ij}^{(BC_{11})}$ үшін $\underset{\sim}{T}_{C_{ECim}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$					$\lambda_{ij}^{(BC_{12})}$ үшін $\underset{\sim}{T}_{C_{ECim}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$					$\lambda_{ij}^{(BC_{13})}$ үшін $\underset{\sim}{T}_{C_{ECim}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$					$\lambda_{ij}^{(BC_{14})}$ үшін $\underset{\sim}{T}_{C_{ECim}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$					$\lambda_{ij}^{(BC_{15})}$ үшін $\underset{\sim}{T}_{C_{ECim}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$				
BC3	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
BC4	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0
BC5	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
BC6	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0

9-кезең - Лингвистикалық танып білу. Соңғы кезеңде ***LR*** терм-жиынтығы арқылы $lr^{(BC_{1bc_1})}$ алынған маңыздылықты лингвистикалық танып білу жүзеге асырылады, мысалы, *m*=5 кезінде (2.6) формуласы бойынша:

$$\underset{\sim}{T}_{LR} = \begin{cases} \text{Ò}^2, & \text{åãåð} \quad lr^{(BC_{1bc_1})} \in [\, lr_{\min}; lr_1[\\ ^2\,\text{Ò}, & \text{åãåð} \quad lr^{(BC_{1bc_1})} \in [\, lr_2; lr_3[\\ ^2\,\hat{I}, & \text{åãåð} \quad lr^{(BC_{1bc_1})} \in [\, lr_4; lr_5[\\ ^2\,Æ, & \text{åãåð} \quad lr^{(BC_{1bc_1})} \in [\, lr_6; lr_7[\\ \hat{I}^{\,2}, & \text{åãåð} \quad lr^{(BC_{1bc_1})} \in [lr_8; lr_{\max}] \end{cases}, \tag{2.6}$$

мұндағы LR ЛА «ҚАТЕР ДЕҢГЕЙІ» терм-жиынтығының мәні арқылы есептелген $lr^{(BC_{1bc_1})}$ көрсетеді. Сонымен бірге (2.7) формуласымен бағаланып жатқан ресурс бойынша $lr^{(cp)}$ орта мәнін есептеуге болады:

$$lr^{(cp)} = (\sum_{bc_1=1}^{m} lr^{(BC_{1bc_1})}) / m. \tag{2.7}$$

1-кезеңде анықталған ***BC1*** және ***BC2*** параметрлері үшін үлгіні қолдана отырып, ақпараттық жүйе ресурсының (белсендінің) пошта серверін қолдану негізінде қатерді бағалау мен анализдеу үлгісін қарастырайық. Олардың идентификациясын сарапшылардың сауалнамасынан құралған сұраныстар көмегімен немесе сарапшылардың пікірі негізінде жиі жүзеге асырады. ISO/IEC 27002 стандартына сәйкес сұраныстар үлгісін келтірейік [8]:

1) Ақпаратты өңдеудің жаңа құралдарын қолдануға қатысты бекітілген, енгізілген, анықталған шешімді қабылдау процедурасы ұйымда бар ма? (стандарттың 6.1.4 пункті) [8]. Осы сұранысқа жауап беру үшін ИӘ немесе ЖОҚ жауаптарының бірін таңдау ұсынылады. Егер сарапшы ИӘ деп жауап берсе, онда бұл процедура кәсіп орында қалай ұйымдастырылды деген айқындау жүргізіледі.

1.1) Ақпаратты өңдеудің жаңа құралдарын мақұлдады ма:

а) тұтынушы басқарма; егер жауап ИӘ болса – онда келесіге өту қажет, егер ЖОҚ болса – онда BC_{1bc_1} $(bc_1 = \overline{1,5})$ барлығы жүзеге асырылуы мүмкін;

б) басқару құралдарының әкімшілігі; егер жауап ИӘ болса – онда келесіге өту қажет, егер ЖОҚ болса – онда BC_{13}- BC_{15} жүзеге асырылуы мүмкін;

в) жергілікті ақпараттық жүйе менеджері; егер жауап ИӘ болса – онда келесіге өту қажет, егер ЖОҚ болса – онда BC_{12} - BC_{15} жүзеге асырылуы мүмкін;

1.2) Жүйенің басқа компоненттерімен қиыстырылуы тексерілді ма? егер жауап ИӘ болса – онда келесіге өту қажет, егер ЖОҚ болса – онда BC_{13}- BC_{15}; жүзеге асырылуы мүмкін;

1.3) Ақпаратты өңдеудің жеке немесе меншікті құралдары: ықшам компьютерлер, үй компьютерлері немесе керек-жарақтар (аспаптар), қолданылады ма, іскерлік ақпаратты өңдеу үшін қажетті бақылау шаралары енгізіліп, анықталған ба? егер жауап ИӘ болса – онда келесіге өту қажет, егер ЖОҚ болса – онда BC_{1bc_1} барлығы жүзеге асырылуы мүмкін;

Егер сарапшы 1-сұранысқа ЖОҚ деп жауап берген жағдай болса, онда ол BC_{17} және BC_1 барлығының жүзеге асырылуына алып келеді.

Берілген сұраныс бойынша сауалнама жүргізіп, жауап нұсқаларын өңдеп шығайық. Айталық, 1-сұранысқа сарапшы оңтайлы жауап берді делік, демек, ол мәліметтерді айқындауға өтті, бұл жерде ол келесі жауапты берді: 1.1а – ИӘ; 1.1б – ИӘ; 1.1в – ЖОҚ; 1.2 ИӘ; 1.3 ЖОҚ.

1-кезең. Сипаттама қорын анықтау мен жауаптарды өңдеуді жүргізейік. Сонымен, берілген белсендіге қатысты $BC_{1bc_1}(bc_1 = \overline{1,n})$ барлығы бағытталған болуы мүмкін, оларды жүзеге асыру кезінде белгілі бір BC_1 басталуы мүмкін, бұл мына тізбектерде суреттелген BC_{11}=>BC_{25}=«ТҚЖБ»; BC_{12}=>BC_{27}=«ҚТҚЖБ»; BC_{13}=>BC_{25}=«ТҚЖБ»; BC_{14}=>BC_{27}=«ҚТҚЖБ»; BC_{15}=>BC_{23}=«ҚЖБ» (мысалы, соңғы тізбек былай түсіндіріледі: пошта серверіне қатысты қызмет көрсетуде бас тартуға және ресурсқа қол жеткізудің бұзуға бастайтын оқиғаға алып келетін әрекет (потенциалды қауіп-қатерлердің жүзеге асуы) жүзеге асуы мүмкін. Міне осылай, берілген белсенді үшін жиынтығы $\boldsymbol{BC_2}$ $BC_2 = \{BC_{23}, BC_{25}, BC_{27}\}$ түрінде беріледі. Қатер дәрежесін бағалау кезінде сәйкес келетін терм-жиынтығы мен маңыздылықтар арақашықтығы бар ЛА қолданамыз, олар мысал түрінде 1-кезеңде қарастырылған.

2-кезең. 1-кезеңнің үлгісінде анықталып, берілген сипаттама қорын пайдаланайық g=4 кезінде, $\boldsymbol{EC}_{Fh\in}\{EC_i\}$={$\boldsymbol{EC_1}$ – ықтималдылық ($\boldsymbol{BC_3}$), $\boldsymbol{EC_2}$ – қауіптілік ($\boldsymbol{BC_4}$), $\boldsymbol{EC_3}$ – жиілік ($\boldsymbol{BC_5}$), $\boldsymbol{EC_4}$ – шығындар ($\boldsymbol{BC_6}$)}, $(i = \overline{1,g})$.

3-кезең. LS бағалауын (2.3) формуласы арқылы жүзеге асырайық: $LS_i = 1/g = 0{,}25$ $(i = \overline{1,4})$.

4-кезең. Қатер деңгей маңыздылығының эталонын анықтау үшін 1-кезеңде берілген үлгіні пайдаланайық, мұндағы [lr_{min}; lr_{max}] [0; 100] сәйкес келеді.

5-кезең. Алдын ала сараптама талдауының негізінде C_{EC_i} этолонды маңыздылығын алдын ала берілген арақашықтығымен аламыз. Ол үшін 1-кезеңде берілген 2.4.-кесте үлгісіндегі мәліметтерден пайдаланайық, мұндағы ***BC5*** компонентін Харрингтон шкаласына негізделіп арақашықтықтарға бөледі [26] , ал ***BC3*** – екі тәртіпке көтерілген мағыналылықтарды үлкейту жолымен оның модификациясына бөледі. ***BC4*** мен ***BC6*** мәндерінің ауқымы сарапшылардың қарауына байланысты анықталады.

6-кезең. Ақпараттық қауіпсіздік белсендісінің кезекті жағдайы сипаттама қорының *ec* мәндерімен әр бірі ***BC1*** мәнімен (2.5-кестеде) сипатталады, бұлар сарапшылардың пікіне негізделіп анықталады. Келесі есептеулерді жүзеге асыру үшін 2.1-кестесінде берілген мәліметтер қолданылады.

7-кезең. BC_{1bc_1} әрбірі үшін ($bc_1 = \overline{1,5}$) (2.4) формула негізінде, берілген ауқымға қатысты (2.4-кестесін қара), бинарлық айнымалы $\lambda_{ij}^{(BC_{1bc_1})}$ көмегімен кезектегі мәндердің $ec_i^{BC_{1bc_1}}$ классификациясы жүзеге асырылады, нақты мәндер 2.7-кестесіне енгізілген.

8-кезең. (2.5) формуласы бойынша ақпараттық қауіпсіздіктің бұзылу қатерінің көрсеткіш деңгейін есептеуді жүргізейік, мұндағы $m = 5$, $j = \overline{1,5}$, $i = \overline{1,4}$, $bc_1 = \overline{1,5}$, lr_1=10, lr_2=30, lr_3=50, lr_4=70, lr_5=90 болса, онда $lr^{(BC_{11})}$ = 0+35+25+0+0=60, $lr^{(BC_{12})}$=60, $lr^{(BC_{13})}$=50, $lr^{(BC_{14})}$=80, $lr^{(BC_{15})}$=50 болады.

9-кезең. Алынған $lr^{(BC_{1bc_1})}$ мәнді лингвистикалық танып білу үшін (2.6) формуласын пайдаланайық. Мұндағы [lr_{min}; lr_{max}] [0; 100] сәкес келеді, ал,

$$\underset{\sim}{T}_{LR} = \begin{cases} \text{Ò²}, & \text{егер} \quad lr^{(BC_{1bc_1})} \in [0;20[\\ \text{² Ò}, & \text{егер} \quad lr^{(BC_{1bc_1})} \in [20;40[\\ \text{² Î}, & \text{егер} \quad lr^{(BC_{1bc_1})} \in [40;60[\\ \text{² Æ}, & \text{егер} \quad lr^{(BC_{1bc_1})} \in [60;80[\\ \text{Î ²}, & \text{егер} \quad lr^{(BC_{1bc_1})} \in [80;100] \end{cases}$$ болады.

Онда $lr^{(BC_{11})}$, $lr^{(BC_{12})}$, $lr^{(BC_{13})}$, $lr^{(BC_{14})}$, $lr^{(BC_{15})}$ көрсеткіштеріне «ҚЖ», «ЖҚ», «ҚО», «ОҚ», «ҚО» ЛА сәйкесінше мәндері анықталған.

Сонымен бірге, берілген белсендіге, (2.7) формуласы бойынша қатер деңгейінің орташа мәні $lr^{(cp)} = (\sum_{bc_1=1}^{5} lr^{(BC_{1bc_1})}) / 5$=(60+60+50+80+50)/5=60 шығарылады да, (2.6) формуласы бойынша оның лингвистикалық эквиваленті – «ЖҚ» анықталады.

Әдісті тексеру мақсатында қатер деңгейі жоғары болған берілген ресурстың қоршаған ортасында ұқсас есептеу жүргізейік яғни сарапшылар тарапынан $\underset{\sim}{T}_{C_{EC_i 4}}$={«Ж»} және $\underset{\sim}{T}_{C_{EC_i 5}}$={«ӨЖ»} деңгейінде BC_{1bc_1} барлығы үшін

$ec_i^{BC_{1bc_1}}$ кезектегі мән бағаланған болатын (1-кезең үлгісін қара). Есептеудің (2.5-кестесімен ұқсастығы бойынша) нәтижесін 2.8-кестесіне енгіземіз.

Кесте 2.8 - 2-үлгі– сипаттама қорының кезектегі мәнін анықтау

EC_i	$ec_i^{BC_{11}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{12}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{13}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{14}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{15}}$	$\underset{\sim}{T}_{C_{EC_i}}$
BC3, (i=1)	80	Ж	79	Ж	95	ӨЖ	86	ӨЖ	71	Ж
BC4, (i=4)	8,4	Ж	9	ӨЖ	7	Ж	8,3	ӨЖ	9	ӨЖ
BC5, (i=2)	0,92	ӨЖ	0,83	Ж	0,9	ӨЖ	0,61	Ж	0,82	Ж
BC6, (i=3)	0,44	ӨЖ	0,39	Ж	0,45	ӨЖ	0,48	Ж	0,43	ӨЖ

Әрі қарай (2.4) формуласы бойынша $ec_i^{BC_{1bc_1}}$ кезектегі мән классификациясы жүргізіліп, нәтижесі 2.9-кестесіне енгізіледі.

Кесте 2.9 - 2 - үлгі– кезекті сипаттама мәндерінің классификациясы

EC_i	$BC_1 \in \{BC_{1bc_1}\}$ $(bc_1 = \overline{1,5})$ үшін λ мәні																									
	$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{11})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{12})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{13})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{14})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4},$ $j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{15})}$					
BC3	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	
BC4	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	
BC5	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	
BC6	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	

$lr^{(BC_{11})}$=85, $lr^{(BC_{12})}$=80, $lr^{(BC_{13})}$=85, $lr^{(BC_{14})}$=80, $lr^{(BC_{15})}$=85 (2.5) формуласы бойынша қатердің көрсеткіш деңгейін есептеуді жүзеге асырайық және алынған нәтижені лингвистикалық танып білу үшін (2.6) формуласын қолданайық сонда барлық $lr^{(BC_{11})}$, $lr^{(BC_{12})}$, $lr^{(BC_{13})}$, $lr^{(BC_{14})}$, $lr^{(BC_{15})}$ көрсеткіштерге ЛА мәндері: «ҚЖ» сәйкес келеді. Әрі қарай қатер деңгейінің $lr^{(cp)}$=(85+80+85+80+85)/5=83 орташа мәні есептеліп, (2.6) формуласы бойынша оның лингвистикалық эквиваленті – «ҚЖ» болып анықталады. Көрініп тұрғандай, қоршаған орта агрессиялығының өсуі кезінде, орташа қатер сияқты, сәйкесінше бөлек мәндер де BC_{1bc_1} $(bc_1 = \overline{1,5})$ бойынша өседі.

2.4 Ақпараттық қауіпсіздікті басқару жүйесі үшін қатерді бағалаудың SecondM әдісі

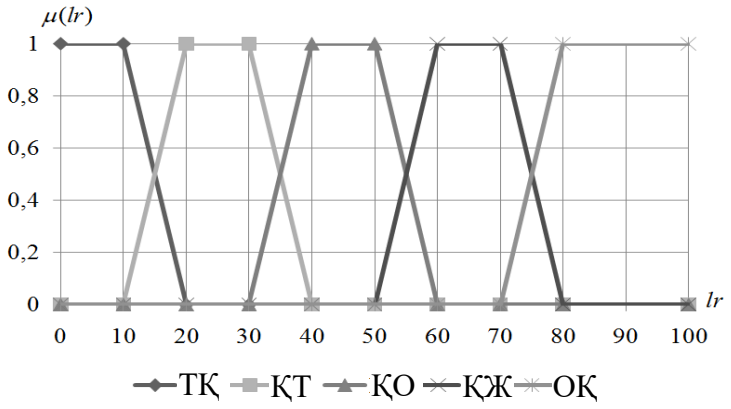
Енді қатерді бағалау деңгейінің мүмкіндіктерін сарапшы барлық уақыт сипаттама қорына қатысты ұнағанын бірдей анықтай алмау шартымен қарастырайық. Бұл мәселені қатерді бағалау мен анализдеу әдісі SecondM (нақты емес) көмегімен шешу ұсынылады. Әдіс құрылымындағы нақты емес сипаттаулар сарапшының күмәніне байланысты туындайды, мұндай күмән әр түрлі классификациялау кезінде пайда болады, мысалы, сарапшы ***BC3*** үшін «жоғары» және «өте жоғары» түсініктер арасында нақты шекара жүргізбейді. Нақты емес сипаттауларды түсіндіру үшін «ҚАТЕР ДЕҢГЕЙІ» ЛА қолданайық, мұндағы $\underset{\sim}{T}_{LR_1}, \ldots, \underset{\sim}{T}_{LR_j}, \ldots, \underset{\sim}{T}_{LR_m}$ трапециялық көріністегі тиістілік функциясымен (ФТ) нақты емес сандар (НЕС) түрінде елестетіледі, сәйкесінше $\mu_1(lr), \ldots, \mu_j(lr), \ldots, \mu_m(lr)$ (2.8) формуласы бойынша есептеледі [81]:

$$\mu_j(lr) = \begin{cases} L\left(\dfrac{b_{1j} - lr}{b_{1j} - a_j}\right), & lr \in [a_j, b_{1j}]; \\ 1, & lr \in [b_{1j}, b_{2j}]; \\ R\left(\dfrac{lr - b_{2j}}{c_j - b_{2j}}\right), & lr \in [b_{2j}, c_j], \end{cases} \qquad (2.8)$$

мұндағы $a_j < b_{1j} \le b_{2j} < c_j$, $j = \overline{1,m}$ кезінде, $\{a_1, c_m\} = \{\varnothing\}$, а $L(lr)$, $R(lr)$ – функциялар (жағымсыз сандар жиынтығында өспейтін), олар $L(-lr) = L(lr)$, $R(-lr) = R(lr)$, $L(0) = R(0) = 1$ ерекшеліктерін қанағаттандырады. Трапециялық түріндегі ФТ $\mu(lr)$ ықшам түрде сипаттау үшін $\tilde{X}_{LR\,j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ түріндегі НЕС-ы трапециялық түрде сипаттау ыңғайлы, мұндағы a_j мен c_j – төменгі ірге абсцистері, ал b_{1j} мен b_{2j} – трапецияның жоғарғы ірге абсцистері (2.1-сурет) ЛА анықталып болған соң сарапшы оны математикалық объект түрінде сәйкес келетін операциялар мен әдістерде қолдана алады. Мұны SecondM үлгісінде көрсетейік.

SecondM әдісі

1-кезең - Лингвистикалық айнымалылар мен нақты емес сандардың ішкі жиынтығын анықтау. Бұл жерде 1-кезеңде FirstM анықталған барлық сипаттамалар қолданылады. Айта кетейік, ***LR***= «ҚАТЕР ДЕҢГЕЙ» ($\boldsymbol{LR} \in \{LR_j\}$) ЛА үшін үлгі түрінде $m = 5$ $\underset{\sim}{T}_{LR_1}$, $\underset{\sim}{T}_{LR_2}$, $\underset{\sim}{T}_{LR_3}$, $\underset{\sim}{T}_{LR_4}$, $\underset{\sim}{T}_{LR_5}$ термдерін қолданайық .



Сурет 2.1 - **LR** ЛА үшін мәндер эталоны

2-кезең мен 3 -кезең FirstM 2 және 3 кезеңдерімен сәйкесінше сәйкес келеді.

4-кезең (Терм-жиынтық санын анықтау) *m*-өлшемді $LR^{(m)}$ ЛА НЕС термдерін $LR^{(m+n)}$-не және $EC_i^{(m)}$ $EC_i^{(m+n)}$-ке эквивалентті қайта жаңғырту үшін қатерді бағалау мен анализдеу тапсырмаларында лингвистикалық айнымалы терм сандарын n-еселі инкременттеу әдістерін қолдану ұсынылады [81]. 2.5 пен 2.6.п.п. әдістер егжей-тегжейлі сипатталады.

5-кезең - Қатер деңгей мәнінің эталонын анықталу. Бұл кезеңде эксперттер өз басымдылығы мен (2.8) формуласы көмегімен арақашықтық мәндеріне қатысты ***LR*** үшін НЕС эталонын анықтайды, олардың саны термдердің қолданылу санына байланысты , мысалы, егер ***LR*** үшін олар *m* болса, онда арақашықтық саны $G=2m-1$ болады, ФТ-мен $\mu_j(lr)$ жалпы түрі мынадай: $[b_{11}; b_{21}[, [b_{21}; b_{12}[, [b_{12}; b_{22}[, \ldots, [b_{2j-1}; b_{1j}[, [b_{1j}; b_{2j}[, \ldots, [b_{2m-1}; b_{1m}[, [b_{1m}; b_{2m}]$ ($j = \overline{1,m}$)

Айталық $m = 5$ болсын, онда $G=9$ болады, ал арақашықтық
$[b_{11}; b_{21}[,[b_{21}; b_{12}[,[b_{12}; b_{22}[,[b_{22}; b_{13}[,[b_{13}; b_{23}[,[b_{23}; b_{14}[,[b_{14}; b_{24}[, [b_{24}; b_{15}[,[b_{15}; b_{25}]$
болады, (2.8) есепке ала отырып сәйкесінше
$[b_{11}; b_{21}[,[a_2, c_1[,[b_{12}; b_{22}[,[a_3; c_2[,[b_{13}; b_{23}[,[a_4; c_3[,[b_{14}; b_{24}[, [a_5; c_4[,[b_{15}; b_{25}]$
болады,
ал қаралып жатқан үлгі үшін нақты мәліметтер (арақашықтық мәндері мен берілген термдердің ФТ) 2.10-кестесіне енгізілген.

Кесте 2.10 - $\mu_j(lr)$ мен арақашықтық мәнінің үлгісі

Арақашықтық	Термдер	$\mu_j(lr)$
$[b_{11}; b_{21}[=[0; 10[$	$\underset{\sim}{T}_{LR_1}$	1
$[b_{21}; b_{12}[=[10; 20[$	$\underset{\sim}{T}_{LR_1}$	$\mu_1(lr) = (20 - lr)/10$
	$\underset{\sim}{T}_{LR_2}$	$\mu_2(lr) = 1 - \mu_1(lr)$

$[b_{12}; b_{22}[=[20; 30[$	$\underset{\sim}{T}_{LR_2}$	1
$[b_{22}; b_{13}[=[30; 40[$	$\underset{\sim}{T}_{LR_2}$	$\mu_2(lr) = (40 - lr) /10$
	$\underset{\sim}{T}_{LR_3}$	$\mu_3(lr) =1- \mu_2(lr)$
$[b_{13}; b_{23}[=[40; 50[$	$\underset{\sim}{T}_{LR_3}$	1
$[b_{23}; b_{14}[=[50; 60[$	$\underset{\sim}{T}_{LR_3}$	$\mu_3(lr) = (60 - lr) /10$
	$\underset{\sim}{T}_{LR_4}$	$\mu_4(lr) =1-\mu_3(lr)$
$[b_{14}; b_{24}[=[60; 70[$	$\underset{\sim}{T}_{LR_4}$	1
$[b_{24}; b_{15}[=[70; 80[$	$\underset{\sim}{T}_{LR_4}$	$\mu_4(lr) = (80 - lr) /10$
	$\underset{\sim}{T}_{LR_5}$	$\mu_5(lr) =1- \mu_4(lr)$
$[b_{15}; b_{25}]=[80; 100]$	$\underset{\sim}{T}_{LR_5}$	1

6-кезең - Сипаттама қорының мәндік эталонын анықтау. Бұл деңгейде сарапшылар FirstM 5-кезеңге ұқсас (2.4-кестесін қара) C_{EC_i} үшін мәндер эталонын анықтау жүргізіледі, бір ерекшелігі бұл жерде берілген мәндерің толық жиынтығы ішкі жиынтық нақты емес сандарға бөлінеді. НЕС арқылы сипаттама қорын ыңғайлы көру үшін 2.11-кестесін қолданайық. Мынадай анықтау үлгісін келтірейік, $\{EC_i\}=\{\boldsymbol{EC_1, EC_2, EC_3, EC_4}\}=\{\boldsymbol{BC_3, BC_4, BC_5, BC_6}\}$ үшін нақты мәліметке ие сандар 2.12-кестесінде берілген. Сонымен бірге $\boldsymbol{BC_3}$, $\boldsymbol{BC_4}$, $\boldsymbol{BC_5}$ мен $\boldsymbol{BC_6}$ үшін НЕС мәні сәйкесінше 2.2-суретінде берілген. Сонымен бірге, C_{EC_i} үшін НЕС $[b_{11}; b_{21}[, [b_{21}; b_{12}[, [b_{12}; b_{22}[, \ldots, [b_{2j-1}; b_{1j}[, [b_{1j}; b_{2j}[, \ldots, [b_{2m-1}; b_{1m}[, [b_{1m}; b_{2m}]$ ($j=\overline{1,m}$) арақашықтық мәндеріне және $\mu_j(c_{EC_i}$ ФТ қатысты беруге болады. Қарастырылып жатқан үлгі үшін m=5 (арақашықтық мәндері мен берілген термдердің ФТ) кезінде нақты мәліметтер 2.13-кестесіне енгізілген.

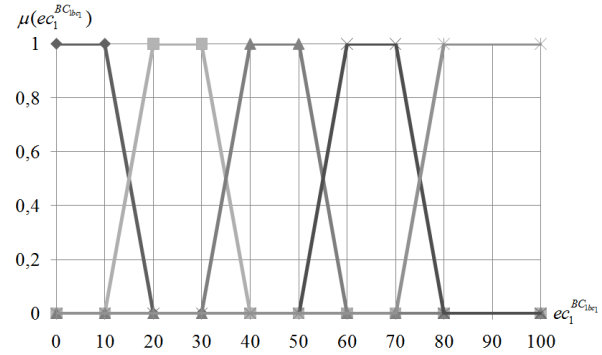
Кесте 2.11 - Сипаттама қорының НЕС мәнін суреттеу

EC_i	$\underset{\sim}{T}_{C_{EC_i1}} - \underset{\sim}{T}_{C_{EC_im}}$ ($j=\overline{1,m}$) үшін НЕС $\underset{\sim}{X}_{C_{EC_ij}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$				
	$\underset{\sim}{T}_{C_{EC_i1}}$	…	$\underset{\sim}{T}_{C_{EC_ij}}$	…	$\underset{\sim}{T}_{C_{EC_im}}$
EC_1	$(a1_{min}; b1_{1min}; b1_{21}; c1)$	…	$(a1_j; b1_{1j}; b1_{2j+1}; c1_{j+1})$	…	$(a1_m; b1_{1m}; b1_{2max}; c1_{max})$
…	…	…	…	…	…
EC_i	$(ai_{min}; bi_{1min}; bi_{21}; ci)$	…	$(ai_j; bi_{1j}; bi_{2j+1}; ci_{j+1})$	…	$(ai_m; bi_{1m}; bi_{2max}; ci_{max})$
…	…	…	…	…	…
EC_g	$(ag_{min}; bg_{1min}; bg_{21}; cg)$	…	$(ag_j; bg_{1j}; bg_{2j+1}; cg_{j+1})$	…	$(ag_m; bg_{1m}; bg_{2max}; cg_{max})$

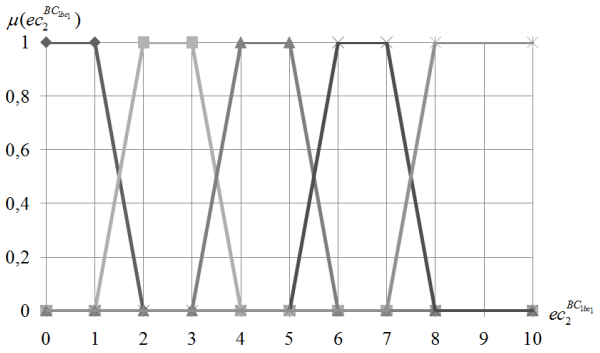
Кесте 2.12 - Сипаттама қорының НЕС мәнін эталонды суреттеу үлгісі

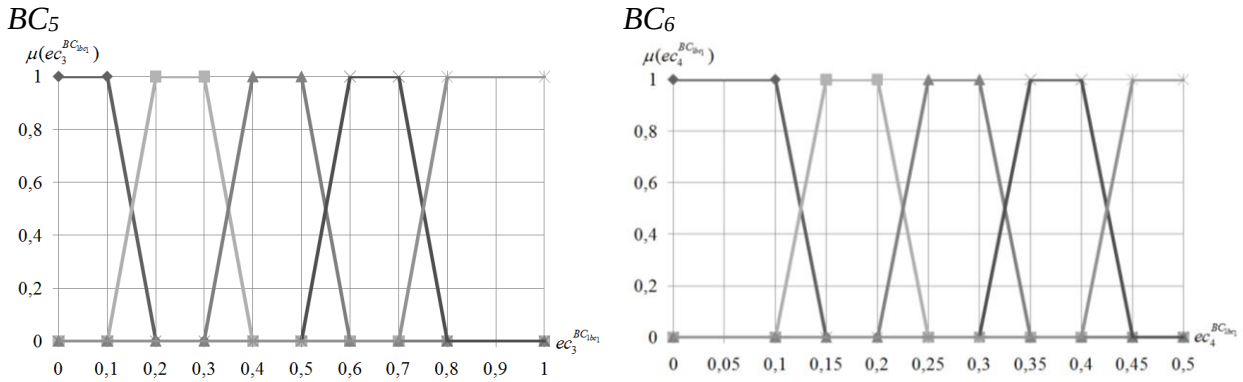
EC_i	$\underset{\sim}{T}_{C_{EC_i1}} - \underset{\sim}{T}_{C_{EC_i5}}$ ($j=\overline{1,5}$) үшін НЕС $\underset{\sim}{X}_{C_{EC_ij}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$				
	$\underset{\sim}{T}_{C_{EC_i1}}$ $(a_1; b_{11}; b_{21}; c_{1)}$	$\underset{\sim}{T}_{C_{EC_i2}}$ $(a_2; b_{12}; b_{22}; c_{2)}$	$\underset{\sim}{T}_{C_{EC_i3}}$ $(a_3; b_{13}; b_{23}; c_{3)}$	$\underset{\sim}{T}_{C_{EC_i4}}$ $(a_4; b_{14}; b_{24}; c_{4)}$	$\underset{\sim}{T}_{C_{EC_i5}}$ $(a_5; b_{15}; b_{25}; c_{5)}$
$EC_1=BC_3$	(0;0;10;20)	(10;20;30;40)	(30;40;50;60)	(50;60;70;80)	(70;80;100;100)
$EC_2=BC_4$	(0;0;1;2)	(1;2;3;4)	(3;4;5;6)	(5;6;7;8)	(7;8;10;10)
$EC_3=BC_5$	(0;0;0,1;0,2)	(0,1;0,2;0,3;0,4)	(0,3;0,4;0,5;0,6)	(0,5;0,6;0,7;0,8)	(0,7;0,8;1;1)
$EC_4=BC_6$	(0;0;0,1;0,15)	(0,1;0,15;0,2;0,25)	(0,2;0,25;0,3;0,35)	(0,3;0,35;0,4;0,45)	(0,4;0,45;0,5;0,5)

BC_3



BC_4





Сурет 2.2 - BC_3, BC_4, BC_5 және BC_6 бағалау компоненттері үшін мәндер эталоны

Кесте 2.13 - $\mu_j(ec_i^{BC_{1bc_1}})$ ($i=\overline{1,4}$, $j=\overline{1,5}$) мен арақашықтық мәнінің үлгісі

EC_i үшін арақашақтық				Терм-дер	$\mu_j(ec_i^{BC_{1bc_1}})$			
BC_3	BC_4	BC_5	BC_6	$\underset{\sim}{T}_{C_{EC_i j}}$	$\mu_j(ec_1^{BC_{1bc_1}})$	$\mu_j(ec_2^{BC_{1bc_1}})$	$\mu_j(ec_3^{BC_{1bc_1}})$	$\mu_j(ec_4^{BC_{1bc_1}})$
[0;10[	[0;1[	[0;0,1[	[0;0,1[	$\underset{\sim}{T}_{C_{EC_i 1}}$	$\mu_1(ec_1^{BC_{1bc_1}})=1$	$\mu_1(ec_2^{BC_{1bc_1}})=1$	$\mu_1(ec_3^{BC_{1bc_1}})=1$	$\mu_1(ec_4^{BC_{1bc_1}})=1$
[10;20[	[1;2[	[0,1;0,2[	[0,1;0,15[	$\underset{\sim}{T}_{C_{EC_i 1}}$	$\mu_1(ec_1^{BC_{1bc_1}})=(20-ec_1^{BC_{1bc_1}})/10$	$\mu_1(ec_2^{BC_{1bc_1}})=(2-ec_2^{BC_{1bc_1}})$	$\mu_1(ec_3^{BC_{1bc_1}})=(0,2-ec_3^{BC_{1bc_1}})*10$	$\mu_1(ec_4^{BC_{1bc_1}})=(0,15-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i 2}}$	$\mu_2(ec_1^{BC_{1bc_1}})=1-\mu_1(ec_1^{BC_{1bc_1}})$	$\mu_2(ec_2^{BC_{1bc_1}})=1-\mu_1(ec_2^{BC_{1bc_1}})$	$\mu_2(ec_3^{BC_{1bc_1}})=1-\mu_1(ec_3^{BC_{1bc_1}})$	$\mu_2(ec_4^{BC_{1bc_1}})=1-\mu_1(ec_4^{BC_{1bc_1}})$
[20;30[	[2;3[	[0,2;0,3[	[0,15;0,2[	$\underset{\sim}{T}_{C_{EC_i 2}}$	$\mu_2(ec_1^{BC_{1bc_1}})=1$	$\mu_2(ec_2^{BC_{1bc_1}})=1$	$\mu_2(ec_3^{BC_{1bc_1}})=1$	$\mu_2(ec_4^{BC_{1bc_1}})=1$
[30;40[	[3;4[	[0,3;0,4[	[0,2;0,25[	$\underset{\sim}{T}_{C_{EC_i 2}}$	$\mu_2(ec_1^{BC_{1bc_1}})=(40-ec_1^{BC_{1bc_1}})/10$	$\mu_2(ec_2^{BC_{1bc_1}})=(4-ec_2^{BC_{1bc_1}})$	$\mu_2(ec_3^{BC_{1bc_1}})=(0,4-ec_3^{BC_{1bc_1}})*10$	$\mu_2(ec_4^{BC_{1bc_1}})=(0,25-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i 3}}$	$\mu_3(ec_1^{BC_{1bc_1}})=1-\mu_2(ec_1^{BC_{1bc_1}})$	$\mu_3(ec_2^{BC_{1bc_1}})=1-\mu_2(ec_2^{BC_{1bc_1}})$	$\mu_3(ec_3^{BC_{1bc_1}})=1-\mu_2(ec_3^{BC_{1bc_1}})$	$\mu_3(ec_4^{BC_{1bc_1}})=1-\mu_2(ec_4^{BC_{1bc_1}})$

[40;50[	[4;5[	[0,4;0,5[	[0,25;0,3[	$\underset{\sim}{T}_{C_{EC_i}3}$	$\mu_3(ec_1^{BC_{1bc_1}})=1$	$\mu_3(ec_2^{BC_{1bc_1}})=1$	$\mu_3(ec_3^{BC_{1bc_1}})=1$	$\mu_3(ec_4^{BC_{1bc_1}})=1$
[50;60[	[5;6[	[0,5;0,6[	[0,3;0,35[	$\underset{\sim}{T}_{C_{EC_i}3}$	$\mu_3(ec_1^{BC_{1bc_1}})=(60-ec_1^{BC_{1bc_1}})/10$	$\mu_3(ec_2^{BC_{1bc_1}})=(6-ec_2^{BC_{1bc_1}})$	$\mu_3(ec_3^{BC_{1bc_1}})=(0,6-ec_3^{BC_{1bc_1}})*10$	$\mu_3(ec_4^{BC_{1bc_1}})=(0,35-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i}4}$	$\mu_4(ec_1^{BC_{1bc_1}})=1-\mu_3(ec_1^{BC_{1bc_1}})$	$\mu_4(ec_2^{BC_{1bc_1}})=1-\mu_3(ec_2^{BC_{1bc_1}})$	$\mu_4(ec_3^{BC_{1bc_1}})=1-\mu_3(ec_3^{BC_{1bc_1}})$	$\mu_4(ec_4^{BC_{1bc_1}})=1-\mu_3(ec_4^{BC_{1bc_1}})$
[60;70[	[6;7[	[0,6;0,7[	[0,35;0,4[	$\underset{\sim}{T}_{C_{EC_i}4}$	$\mu_4(ec_1^{BC_{1bc_1}})=1$	$\mu_4(ec_2^{BC_{1bc_1}})=1$	$\mu_4(ec_3^{BC_{1bc_1}})=1$	$\mu_4(ec_4^{BC_{1bc_1}})=1$
[70;80[	[7;8[	[0,7;0,8[	[0,4;0,45[	$\underset{\sim}{T}_{C_{EC_i}4}$	$\mu_4(ec_1^{BC_{1bc_1}})=(80-ec_1^{BC_{1bc_1}})/10$	$\mu_4(ec_2^{BC_{1bc_1}})=(8-ec_2^{BC_{1bc_1}})$	$\mu_4(ec_3^{BC_{1bc_1}})=(0,8-ec_3^{BC_{1bc_1}})*10$	$\mu_4(ec_4^{BC_{1bc_1}})=(0,45-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i}5}$	$\mu_5(ec_1^{BC_{1bc_1}})=1-\mu_4(ec_1^{BC_{1bc_1}})$	$\mu_5(ec_2^{BC_{1bc_1}})=1-\mu_4(ec_2^{BC_{1bc_1}})$	$\mu_5(ec_3^{BC_{1bc_1}})=1-\mu_4(ec_3^{BC_{1bc_1}})$	$\mu_5(ec_4^{BC_{1bc_1}})=1-\mu_4(ec_4^{BC_{1bc_1}})$
[80;100]	[8;10[	[0,8;1[	[0,45;0,5[	$\underset{\sim}{T}_{C_{EC_i}5}$	$\mu_5(ec_1^{BC_{1bc_1}})=1$	$\mu_5(ec_2^{BC_{1bc_1}})=1$	$\mu_5(ec_3^{BC_{1bc_1}})=1$	$\mu_5(ec_4^{BC_{1bc_1}})=1$

7-кезең - Сипаттаманың кезектегі мәнін бағалау. FirstM 6-кезеңімен сәйкес келеді.

8-кезең - Кезектегі мәндердің классификациясы. Бұл кезеңде сарапшылар қисынына келтірген эталонды мәндер көмегімен (2.2 сурет) берілген НЕС-ға $ec_i^{BC_{1bc_1}}$ тиістілігі анықталады да, бұл бойынша (2.9) формуласының көмегімен λ мәні қалыптасады. Ыңғайлы болу үшін жүргізілген есептердің нәтижелері 2.6-кестесіне енгізіледі, мұндағы $\lambda_{ij}^{(BC_{1bc_1})} - \underset{\sim}{T}_{C_{EC_i j}}$ нақты емес ішкі жиынтыққа $ec_i^{BC_{1bc_1}}$ тасымалдаушы тиістілігінің деңгейі.

$$\lambda_{i1}^{(BC_{1bc_1})}=\begin{cases}1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{11},bi_{12}[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[bi_{11},ci_1[;\\ \mu_1(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{12},ci_1[,\end{cases}\qquad \lambda_{ij}^{(BC_{1bc_1})}=\begin{cases}\mu_j(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[ai_j,bi_{1j}[;\\ 1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{1j},bi_{2j}[;\\ \mu_j(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{2j},ci_j[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[ai_j,ci_j[,\end{cases}\qquad (2.9)$$

$$\lambda_{im}^{(BC_{1bc_1})}=\begin{cases}\mu_m(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[ai_m,bi_{1m}[;\\ 1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{1m},bi_{2m}[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[ai_m,bi_{2m}[,\end{cases}\qquad (j=\overline{2,m-1}).$$

9-кезең - Қатер деңгейін бағалау. FirstM 8-кезеңмен сәйкес келеді.

10-кезең - Қатердің құрылымдасқан параметрін қалыптастыру. (2.1 суретінде, (2.8)) құрылған эталондар және есептелген $lr^{(BC_{1bc_1})}$ мәні негізінде (2.10) формуласы бойынша *SP* қатердің құрылымдасқан параметрін қалыптастырамыз:

$$SP^{(BC_{1bc_1})}=\begin{cases}(lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j})\ егер\ \ \mu_j(lr)=1;\\ (lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j}(\mu_j(lr));\underset{\sim}{T}_{LR_{j+1}}(\mu_{j+1}(lr)))\ егер\ \ \mu_j(lr),\mu_{j+1}(lr)\neq 1,\end{cases}\qquad (2.10)$$

мұндағы $lr^{(BC_{1bc_1})}$ эквивалент саны $\underset{\sim}{T}_{LR_j}$ – қатер деңгейі, сияқты, $(lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j})$ ауызша түсіндіріледі, ал $(lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j}(\mu_j(lr));\underset{\sim}{T}_{LR_{j+1}}(\mu_{j+1}(lr)))$ - $lr^{(BC_{1bc_1})}$ эквивалент саны қатер деңгейі сияқты $\underset{\sim}{T}_{LR_j}\mu_j(lr)$ және $\underset{\sim}{T}_{LR_{j+1}}\mu_{j+1}(lr)$ шекарасында сарапшының сенімділігімен $\underset{\sim}{T}_{LR_j}$ және $\underset{\sim}{T}_{LR_{j+1}}$ арасында шектеседі.

SP көмегімен қатер деңгейінің сандық мәні мен $\lambda_{ij}^{(BC_{1bc_1})}$ параметрі арқылы әрі қарай классификациялаумен сипаттама қорының кезектегі мәнін қалыптастыру кезінде сарапшының сенімсіздігін есепке алатын лингвистикалық түсіндірілуін алуға болады.

Нақты үлгідегі әдіс жұмысын қарастырайық. FirstM-не ұқсас сол бір белсенді мен $\boldsymbol{BC_1}$ және $\boldsymbol{BC_2}$ жиынтықтарын қолданайық. 2.13-кестесі мен (2.9) формуласының критериясы бойынша кезекті $ec_i^{BC_{1bc_1}}$ мәндерінің классификациясын жүргізейік. BC_{1bc_1} үшін $(bc_1=\overline{1,5})$ болады, (2.9) формуласы келесі түрге ие:

$$\lambda_{i1}^{(BC_{1bc_1})}=\begin{cases}1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{11},bi_{21}[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[bi_{11},ci_1[;\\ \mu_1(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{12},ci_1[,\end{cases}\qquad \lambda_{i2}^{(BC_{1bc_1})}=\begin{cases}\mu_2(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[ai_2,bi_{12}[;\\ 1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{12},bi_{22}[;\\ \mu_2(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{22},ci_2[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[ai_2,ci_2[,\end{cases}$$

$$\lambda_{i3}^{(BC_{1bc_1})}=\begin{cases}\mu_3(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[ai_3,bi_{13}[;\\ 1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{13},bi_{23}[;\\ \mu_3(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{23},ci_3[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[ai_3,ci_3[,\end{cases}\quad \lambda_{i4}^{(BC_{1bc_1})}=\begin{cases}\mu_4(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[ai_4,bi_{14}[;\\ 1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{14},bi_{24}[;\\ \mu_4(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{24},ci_4[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[ai_4,ci_4[,\end{cases}$$

$$\lambda_{i5}^{(BC_{1bc_1})}=\begin{cases}\mu_5(ec_i^{BC_{1bc_1}})\ егер\ \ ec_i^{BC_{1bc_1}}\in[ai_5,bi_{15}[;\\ 1\ егер\ \ ec_i^{BC_{1bc_1}}\in[bi_{15},bi_{25}[;\\ 0\ егер\ \ ec_i^{BC_{1bc_1}}\notin[ai_5,bi_{25}[.\end{cases}$$

ал оның көмегімен есептелген мәндер 2.6-кестесі негізінде 2.14-кестесіне енгізіледі.

Кесте 2.14 - 1 Үлгі – кезекті сипаттама мәнінің классификациясы

EC_i	$BC_1\in\{BC_{1bc_1}\}$ $(bc_1=\overline{1,5})$ үшін λ мәні																									
	$\underset{\sim}{T}_{C_{EC_im}}$ $(i=\overline{1,4},\ j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{11})}$					$\underset{\sim}{T}_{C_{EC_im}}$ $(i=\overline{1,4},\ j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{12})}$					$\underset{\sim}{T}_{C_{EC_im}}$ $(i=\overline{1,4},\ j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{13})}$					$\underset{\sim}{T}_{C_{EC_im}}$ $(i=\overline{1,4},\ j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{14})}$					$\underset{\sim}{T}_{C_{EC_im}}$ $(i=\overline{1,4},\ j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{15})}$				
BC_3	0	0	0	0,8	0,2	0	0	0,2	0,8	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
BC_4	0	0	0,6	0,4	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0,5	0,5	0
BC_5	0	0	0	0,8	0,2	0	0	0,2	0,8	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
BC_6	0	0,4	0,6	0	0	0	0	0,4	0,6	0	0	1	0	0	0	0	0	0	1	0	0	0,2	0,8	0	0

Енді (2.5) формуласы бойынша АҚ қатерінің деңгейін бағалауды жүзеге асырайық. Нәтижесінде келесі мәндерді аламыз: $lr^{(BC_{11})}$=62, $lr^{(BC_{12})}$=66, $lr^{(BC_{13})}$=50, $lr^{(BC_{14})}$=75, $lr^{(BC_{15})}$=61,5 және әрі қарай (2.8) мен (2.10) негізінде $SP^{(BC_{1bc_1})}$: $SP^{(BC_{11})}=(lr^{(BC_{11})};\underset{\sim}{T}_{LR_4})$=(62; ҚЖ), $SP^{(BC_{12})}=(66;$ ҚЖ), $SP^{(BC_{13})}=(50;$ ҚО),

$SP^{(BC_{14})}=(lr^{(BC_{14})};\underset{\sim}{T}_{LR_4}(\mu_4(lr));\underset{\sim}{T}_{LR_5}(\mu_5(lr)))$=(75; ҚЖ(0,5); ПҚ(0,5)), $SP^{(BC_{15})}=(61{,}5;$ ҚЖ) қалыптасады, мұндағы, мысалы, 62 эквивалент санымен жоғары деңгейлі қатер сияқты (62; ҚЖ) ауызша түсіндіріледі, ал (75; ҚЖ (0,5); ЖҚ(0,5)) 75 эквивалент санымен қатер деңгейі сияқты сарапшы сенімділігімен ҚЖ – 0,5 және ЖҚ – 0,5 шекарасы бойынша жоғары қатер мен өте жоғары қатер арасында шектеседі.

Сонымен бірге, FirstM (9-кезеңіне) ұқсастығы бойынша (2.7) формуласы негізінде берілген белсенді үшін қатер деңгейінің оташа мәнін есептеуге

болады: $lr^{(cp)}$=(62+66+50+75+61,5)/5=62,9 және ол үшін $SP^{(cp)}$= (62,9; ҚЖ) құруға болады.

Есептеуді берілген ресурсты қоршаған ортада жоғары қатер деңгейімен (FirstM 2.8-кестесіндегі мәліметтер негізінде) барабар орындайық. Кезектегі сипаттама қорының классификациясын жүзеге асырайық, ал нәтижелерін 2.15-кестесіне енгіземіз.

Кесте 2.15 - 2-үлгі – кезектегі сипаттама мәндерінің классификациясы

EC_i	$BC_1 \in \{BC_{1bc_1}\}$ $(bc_1 = \overline{1,5})$ үшін λ мәні																								
	$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{11})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{12})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{13})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{14})}$					$\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$ үшін $\lambda_{ij}^{(BC_{15})}$				
BC_3	0	0	0	0	1	0	0	0	0,1	0,9	0	0	0	0	1	0	0	0	0	1	0	0	0	0,9	0,1
BC_4	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1
BC_5	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1
BC_6	0	0	0	0,2	0,8	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0,4	0,6

(2.5) формуласы бойынша қатер деңгейін шығарамыз, нәтижеде мына мәндерді аламыз: $lr^{(BC_{11})}$=89, $lr^{(BC_{12})}$=84,5, $lr^{(BC_{13})}$=85, $lr^{(BC_{14})}$=85, $lr^{(BC_{15})}$=83,4, $SP^{(BC_{11})}$ =(89; ӨЖҚ), $SP^{(BC_{12})}$=(84,5; ӨЖҚ), $SP^{(BC_{13})}$=(85; ӨЖҚ), $SP^{(BC_{14})}$=(85; ӨЖҚ), $SP^{(BC_{15})}$ =(83,4; ӨЖҚ), сонымен бірге $lr^{(cp)}$=(89+84,5+85+85+83,4)/5=85,4 мен $SP^{(cp)}$ =(85,4; ӨЖҚ) анықталады.

Көрініп тұрғандай, қоршаған орта агрессиясының өсуі кезінде сәйкесінше орташа қатер «ЖҚ-ден» «ӨЖҚ-ге» дейін өссе, BC_{1bc_1} $bc_1 = \overline{1,5}$ бойынша бөлек мәндері де өсті, мысалы, – BC_{11} «ҚЖ»-нан «ӨЖҚ»-ге дейін. Сонымен бірге, айта кететін жайт, сенімсіздік аймақты жағдайы кезінде (сарапшылар өз артықшылығының бір мағыналылығына күмән тудырған кезде) SecondM қатерді әрі қарай өңдеу кезінде сарапшыға фиксацияланған көрсеткіш мәнін және сәйкес келтін шешімдерді қабылдау бойынша мүмкін болған арақашықтықты қолдануға мүмкіндік береді.

Қатер сипаттама қорының кортеж моделі негізінде өңделген әдістер ҚБАҚ-ын жасауға мүмкіндік береді. ҚБАҚ басқа (2.2 п.) белгілілерге қарағанда, кіріс мәліметтері түрінде әртүрлі сипаттама қор жиынын қолданады (мысалы, **BC_3, BC_4, BC_5** пен **BC_6** кез келген қиыстырулары мен үйлестірулері), бұл өз кезегінде детерминдендірілгенде де, төмен нысандандырылған нақты емес анықталған ортада жұмыс істейтін жобаланушы құралдарды бағалау мүмкіндіктерін кеңейтіп, икемділігін көтеруге мүмкіндік береді.

2.5 Лингвистикалық айнымалы терм сандарын n-еселі инкременттеу әдісі

Нақты емес логикаға негізделетін АҚ ҚБАҚ-ы бар. Олар жүйені реттеу барысында қор көлемін инициализациялау кезеңінде сарапшылар анықтаған терм-жиынтықтың фиксациялық санды ЛА қолданады.

Мақсатымыз әдісті өңдеу болып табылып, ол АҚ қатерін бағалау мен анализдеу мәселелерін шешу кезінде эквивалентті түрде n-еселі инкременттелген ЛА тәртібін (термдер саны) алдын ала анықтауға мүмкіндік береді. Бұл көрсетілген жүйенің әрі қарай дамуы мен мүмкіндіктерінің кеңейуіне септігін тигізеді. Әдіс қалыптастыру, кеңейту және жеке қорды кеңейтумен байланысты үш кезеңнен тұрады.

1-кезең – Қорды рәсімдеу. Қойылған мақсатқа жету үшін лингвистикалық айнымалының терм сандарын n-еселі инкременттеу әдісін оның бір тәртіпті плюске трансформациалану қызметі негізінде қолданамыз, ол FT^{+1} ***(ЛА)*** түрінде белгіленеді. ЛА түрінде *LR* – «ҚАТЕР ДЕҢГЕЙІН» қолданайық (2.3 п.). Базалық формуланы шығару үшін бір тәртіпке $\boldsymbol{LR}^{(m)}$ (*m* – терм-жиынтық саны) көтерудің *n*-мүшелерінен бірізділікті қолданамыз яғни:

$$\begin{cases} LR^{(m+1)} = FT^{+1}(LR^{(m)}); \\ LR^{(m+2)} = FT^{+1}(LR^{(m+1)}); \\ LR^{(m+3)} = FT^{+1}(LR^{(m+2)}); \\ \ldots \\ LR^{(m+n)} = FT^{+1}(LR^{(m+n+1)}). \end{cases} \tag{2.11}$$

(2.11) формуласында сәйкесінше ауыстырып қоюды орындай отырып, мынаны аламыз:

$$\begin{cases} LR^{(m+2)} = FT^{+1}(FT^{+1}(LR^{(m)})); \\ LR^{(m+3)} = FT^{+1}(FT^{+1}(FT^{+1}(LR^{(m)}))); \\ \ldots \\ LR^{(m+n)} = \underbrace{FT^{+1}(\ldots FT^{+1}(FT^{+1}(FT^{+1}}_{n}(LR^{(m)})))\ldots). \end{cases} \tag{2.12}$$

FT^{+1} ЛА инкременттеу қызметін жүзеге асыру үшін n-еселі бірізділікті FT^{+n} арқылы белгілесек, онда (2.12) формуласын келесі түрде елестетуге болады:

$$\begin{cases} LR^{(m+2)} = FT^{+2}(LR^{(m)}); \\ LR^{(m+3)} = FT^{+3}(LR^{(m)}); \\ \ldots \\ LR^{(m+n)} = FT^{+n}(LR^{(m)}). \end{cases} \tag{2.13}$$

Міне осылай, (2.13) формуласында елестетілетін соңғы жазбаны мына түрде:

$$LR^{(m+n)} = FT^{+n}(LR^{(m)}), \tag{2.14}$$

ЛА n-еселі (+n) тәртіпке инкременттеу үшін басты формула (немесе база) түрінде анықтаймыз.

2-кезең – Қордың кеңейуі. ЛА ($\boldsymbol{LR}^{(m)}$) терм жиынынан тұратынын есепке алсақ (2.4 п.), онда (2.11) формуласын келесі түрде елестетуге болады:

$$\begin{cases} LR^{(m+1)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_m}, T_{\sim LR_{m+1}}) = FT^{+1}(LR^{(m)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m-1}}, T_{\sim LR_m})); \\ LR^{(m+2)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim DR_{m+1}}, T_{\sim LR_{m+2}}) = FT^{+1}(LR^{(m+1)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_m}, T_{\sim LR_{m+1}})); \\ LR^{(m+3)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+2}}, T_{\sim LR_{m+3}}) = FT^{+1}(LR^{(m+2)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+1}}, T_{\sim LR_{m+2}})); \\ ... \\ LR^{(m+n)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+n-1}}, T_{\sim LR_{m+n}}) = FT^{+1}(LR^{(m+n-1)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+n-2}}, T_{\sim LR_{m+n-1}})). \end{cases} \quad (2.15)$$

(2.15) формуласында сәйкесінше ауыстырып қоюды орындай отырып, мынаны аламыз:

$$\begin{cases} LR^{(m+2)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+1}}, T_{\sim LR_{m+2}}) = FT^{+2}(LR^{(m)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m-1}}, T_{\sim LR_m})); \\ LR^{(m+3)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+2}}, T_{\sim LR_{m+3}}) = FT^{+3}(LR^{(m)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m-1}}, T_{\sim LR_m})); \\ ... \\ LR^{(m+n)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+n-1}}, T_{\sim LR_{m+n}}) = FT^{+n}(LR^{(m)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m-1}}, T_{\sim LR_m})). \end{cases} \quad (2.16)$$

Міне осылай, (2.16) формуласындағы соңғы аналитикалық мәндерді

$$LR^{(m+n)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m+n-1}}, T_{\sim LR_{m+n}}) = FT^{+n}(LR^{(m)}(T_{\sim LR_1}, T_{\sim LR_2}, ..., T_{\sim LR_{m-1}}, T_{\sim LR_m})), \quad (2.17)$$

(2.14) басты формуланың кеңейуі түрінде анықтайық.

3-кезең – Қордың жиі кеңейуі. Себебі, $LR^{(m)}$ ЛА-да НЕС әр түрлі $\mu(lr)$ тиістілік функциясымен (ФТ) [82-84] беріледі, ал мұндай ФТ-ді ықшам сипаттау мақсатында $\tilde{X}_{LR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ түріндегі НЕС-ды трапеция түрінде сипаттау ыңғайлы, мұндағы a_j және c_j – трапецияның төменгі ірге абсцистері, ал b_{1j} және b_{2j} – трапецияның жоғарғы ірге абсцистері [82-84] ($j = \overline{1,m}$ кезінде) болса, онда (2.17) формуласын былай береміз де:

$$LR^{(m+n)}((a_1, b_{11}, b_{21}, c_1), (a_2, b_{12}, b_{22}, c_2), ..., (a_{m+n-1}, b_{1m+n-1}, b_{2m+n-1}, c_{m+n-1}), (a_{m+n}, b_{1m+n}, b_{2m+n}, c_{m+n})) = FT^{+n}(LR^{(m)}((a_1, b_{11}, b_{21}, c_1), (a_2, b_{12}, b_{22}, c_2), ..., (a_{m-1}, b_{1m-1}, b_{2m-1}, c_{m-1}), (a_m, b_{1m}, b_{2m}, c_m))) \quad (2.18)$$

оны қорды ең бірінші жеке кеңейту деп атайық.

Әдіс жұмысын нақты үлгіде қарастырайық та, оның негізіне қордың бірінші жеке кеңейуін қояйық. Әрі қарай өзгеру мүмкіндігін есепке ала отырып бастапқы мәліметтер $m=3$ түрінде таралу кезінде (2.16-кестесін қара) кезінде бірқалыпты, бірқалыпты емес, өсуші, азаймалы таралу типтерімен трапециялық эталонды НЕС қолданамыз.

Кесте 2.16 - *m*=3 кезінде эталонды,трапециялық НЕС үлгісі

LR ЛА НЕС таралу типтері	НЕС $\underset{\sim}{T}_{LR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ $(j=\overline{1,3})$		
	$\underset{\sim}{T}_{LR_1}$	$\underset{\sim}{T}_{LR_2}$	$\underset{\sim}{T}_{LR_3}$
Бірқалыпты	$(0; 0; 20; 40)_{LR}$	$(20; 40; 60; 80)_{LR}$	$(60; 80; 100; 100)_{LR}$
Бірқалыпты емес	$(0; 0; 18; 35)_{LR}$	$(18; 35; 60; 85)_{LR}$	$(60; 85; 100; 100)_{LR}$
Өсуші	$(0; 0; 3; 16)_{LR}$	$(3; 16; 33; 65)_{LR}$	$(33; 65; 100; 100)_{LR}$
Азаймалы	$(0; 0; 28; 51)_{LR}$	$(28; 51; 71; 87)_{LR}$	$(71; 87; 100; 100)_{LR}$

n=$\overline{2,3}$ кезіндегі сәйкес келетін қайта жаңғыртуларды жүзеге асырайық. Жалпы функцияны айтарлықтай қиын болғандықтан интеграция түріндегі қайта жаңғыртуларды жүзеге асырайық. Сондықтан (2.12) формуласымен қолдану орынды. n=2 болсын, ал m=3 болсын (m – ЛА-ғы термден саны), онда (2.12) формуласы мына түрге ие болады:

$$LR^{(5)} = FT^{+1}(FT^{+1}(LR^{(3)})),$$

ал (2.17) формуласы келесі түрге ие болады:

$$LR^{(5)}(\underset{\sim}{T}_{LR_1}, \underset{\sim}{T}_{LR_2}, \underset{\sim}{T}_{LR_3}, \underset{\sim}{T}_{LR_4}, \underset{\sim}{T}_{LR_5}) = FT^{+1}(FT^{+1}(LR^{(3)}(\underset{\sim}{T}_{LR_1}, \underset{\sim}{T}_{LR_2}, \underset{\sim}{T}_{LR_3}))),$$

мұндағы

$$\underset{\sim}{T}_{LR}^{(3)} = \left\{ \bigcup_{j=1}^{3} \underset{\sim}{T}_{LR_j} \right\} = \left\{ \underset{\sim}{T}_{LR_1}, \underset{\sim}{T}_{LR_2}, \underset{\sim}{T}_{LR_3} \right\} = \left\{ \underset{\sim}{\text{ò}}, \underset{\sim}{\hat{\imath}}, \underset{\sim}{\text{æ}} \right\}, \ j=\overline{1,3}, \qquad (2.19)$$

ал ҚТ – «АҚ бұзылу қатерінің деңгейі төмен», ҚО - «АҚ бұзылу қатерінің деңгейі орташа», ҚЖ - «АҚ бұзылу қатерінің деңгейі жоғары», сонымен бірге

$$\underset{\sim}{T}_{LR}^{(5)} = \left\{ \bigcup_{j=1}^{5} \underset{\sim}{T}_{LR_j} \right\} = \left\{ \underset{\sim}{T}_{LR_1}, \underset{\sim}{T}_{LR_2}, \underset{\sim}{T}_{LR_3}, \underset{\sim}{T}_{LR_4}, \underset{\sim}{T}_{LR_5} \right\} = \left\{ \underset{\sim}{\text{ò}^2}, \underset{\sim}{\text{ò}}, \underset{\sim}{\hat{\imath}}, \underset{\sim}{\text{æ}}, \underset{\sim}{\text{æ}^2} \right\}, \qquad (2.20)$$

ал ТҚ - «АҚ бұзылу қатерінің өте төмен деңгейі», ҚТ – «АҚ бұзылу қатерінің төмен деңгейі», ҚО - «АҚ бұзылу қатерінің орташа деңгейі», ҚЖ - «АҚ бұзылу қатерінің жоғары деңгейі», ШЖҚ - «АҚ бұзылу қатерінің шегіне жеткен деңгейі». Осыдан шыға отырып (2.18) формуласын келесі түрде беруге болады:

$$LR^{(5)}((a_1,b_{11},b_{21},c_1),(a_2,b_{12},b_{22},c_2),(a_3,b_{13},b_{23},c_3),(a_4,b_{14},b_{24},c_4),(a_5,b_{15},b_{25},c_5)) = FT^{+1}(FT^{+1}(LR^{(3)}((a_1,b_{11},b_{21},c_1),(a_2,b_{12},b_{22},c_2),(a_3,b_{13},b_{23},c_3)))). \qquad (2.21)$$

1-үлгі –бірқалыпты таралу типі. (2.19) формуласындағы термдермен $\boldsymbol{LR}^{(3)}$ ЛА анықталып жатқан болсын. $\underset{\sim}{T}_{LR_j}$, $j=\overline{1,3}$ сандық мәндерін анықтау үшін

2.16 -кестедегі НЕС бірқалыпты таралуы типтері бар мәліметтерді қолданайық яғни олар үшін бірқалыптылық шарттығы шындық болады:

$\Omega_p = (b_{21} - b_{11} = b_{22} - b_{12}) \wedge (b_{22} - b_{12} = b_{23} - b_{13}) \wedge (b_{12} - b_{21} = b_{13} - b_{22})$=(20–0=60–40) ∧ (60–40=100–80) ∧ (40–20=80–60)=1 ∧ 1 ∧ 1=1. Көрініп тұрғандай,

бірқалыптылық шарттығы шындық ($\Omega_p = 1$), сондықтан НЕС $\boldsymbol{LR}^{(3)}$ ЛА бірқалыпты таралу типіне сәйкес келеді (2.3-суретін қара, *а, б* және 2.16, 2.17-кестелер.).

Қажетті кезеңдерді орындау арқылы (2.18) функциясын жүзеге асыру үшін n=2 кезінде $\boldsymbol{LR}^{(3)}$ ЛА (2.21) берілгенді n-еселі инкременттеуді жүзеге асыру қажет. 2-тәртіпке инкременттеуді 2-еселі итерация арқылы жүзеге асырамыз.

1-кезең. Түзетуші параметрлерді анықтау үшін (2.22) және (2.23) формулаларын қолданайық:

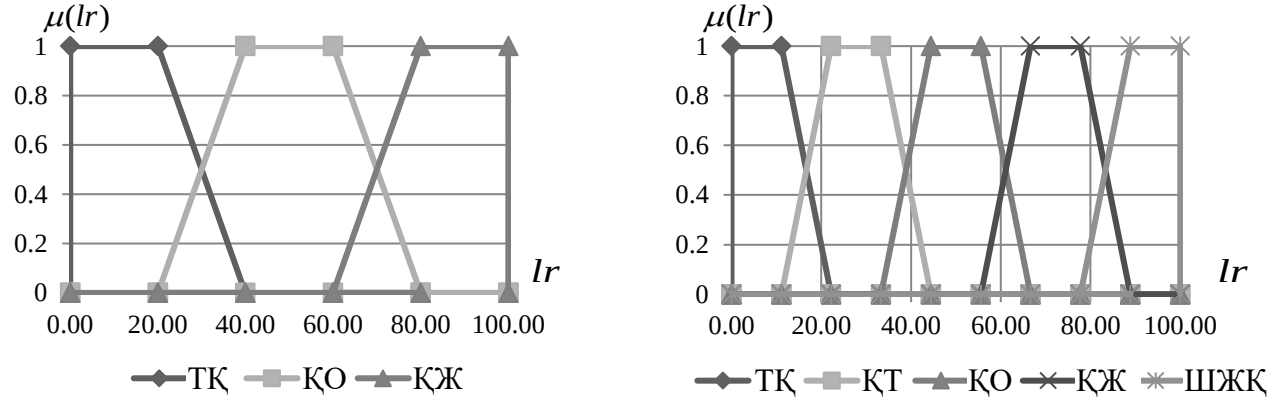
$$k_1^{(m+1)} = \frac{\sum_{j=1}^{m}\left(b_{2j}^{(m)} - b_{1j}^{(m)}\right)}{m},\ k_2^{(m+1)} = \frac{\sum_{j=2}^{m}\left(b_{1j}^{(m)} - b_{2j-1}^{(m)}\right)}{m-1},\ k^{(m+1)} = k_1^{(m+1)} + k_2^{(m+1)},\ j = \overline{1,m}; \quad (2.22)$$

$$l_1^{(m+1)} = \frac{a_2^{(m)} - a_1^{(m)} + \sum_{j=3}^{m}\left(a_j^{(m)} - c_{j-2}^{(m)}\right) + c_m^{(m)} - c_{m-1}^{(m)}}{m},\ l_2^{(m+1)} = \frac{\sum_{j=2}^{m}\left(c_{j-1}^{(m)} - a_j^{(m)}\right)}{m-1},\ l^{(m+1)} = l_1^{(m+1)} + l_2^{(m+1)}, \quad (2.23)$$

мұндағы $k_1^{(m+1)}, k_2^{(m+1)}, k^{(m+1)}$ мен $l_1^{(m+1)}$, $l_2^{(m+1)}$, $l^{(m+1)}$ - түзетуші параметрлер сәйкесінше жоғарғы және төменгі абсцистер іргетасы үшін трапециялар, ал *m* - бастапқы терм-жиынтықтар саны.

Бірінші итерация: $k_1^{(4)} = \left(b_{21}^{(3)} - b_{11}^{(3)} + b_{22}^{(3)} - b_{12}^{(3)} + b_{23}^{(3)} - b_{13}^{(3)}\right)/3 =$ (20 – 0 + 60 – 40 + 100 – 80) / 3 = 20, $k_2^{(4)} = \left(b_{12}^{(3)} - b_{21}^{(3)} + b_{13}^{(3)} - b_{22}^{(3)}\right)/2 =$ (40– 20 + 80 – 60)/2 = 20, $k^{(4)} = k_1^{(4)} + k_2^{(4)} =$ 20 + 20 = 40,

$l_1^{(4)} = \left(a_2^{(3)} - a_1^{(3)} + a_3^{(3)} - c_1^{(3)} + c_3^{(3)} - c_2^{(3)}\right)/3 =$ (20 – 0 + 60 – 40 + 100 – 80) / 3 = 20, $l_2^{(4)} = \left(c_1^{(3)} - a_2^{(3)} + c_2^{(3)} - a_3^{(3)}\right)/2 =$(40 – 20 + 80 – 60)/2 = 20, $l^{(4)} = l_1^{(4)} + l_2^{(4)} =$ 20 + 20 = 40.



а) б)

Сурет 2.3 - ***LR*** ЛА үшін бірқалыпты таралған НЕС эталонды мәндер термдері а) $\underset{\sim LR}{T}^{(3)}$; б) $\underset{\sim LR}{T}^{(5)}$

Екінші итерация: $k_1^{(5)} = \left(b_{21}^{(4)} - b_{11}^{(4)} + b_{22}^{(4)} - b_{12}^{(4)} + b_{23}^{(4)} - b_{13}^{(4)} + b_{24}^{(4)} - b_{14}^{(4)}\right)/4 =$ (14,29 – 0 + 42,86 – 28,57 + 71,43 – 57,16 + 100,0 – 85,71) / 4 = 14,29, $k_2^{(5)} =$

$\left(b_{12}^{(4)} - b_{21}^{(4)} + b_{13}^{(4)} - b_{22}^{(4)} + b_{14}^{(4)} - b_{23}^{(4)}\right)/3 =$ (28,57 – 14,29 + 57,14 – 42,86 + 85,71 – 71,43)/3 = 14,29, $k^{(5)} = k_1^{(5)} + k_2^{(5)} =$ 14,29 + 14,29 = 28,58,

$l_1^{(5)} = \left(a_2^{(4)} - a_1^{(4)} + a_3^{(4)} - c_1^{(4)} + a_4^{(4)} - c_2^{(4)} + c_4^{(4)} - c_3^{(4)}\right)/4 =$ (14,29 – 0 + 42,86 – 28,57 + 71,43 – 57,14 + 100,0 – 85,71) / 4 = 14,29, $l_2^{(5)} = \left(c_1^{(4)} - a_2^{(4)} + c_2^{(4)} - a_3^{(4)} + c_3^{(4)} - a_4^{(4)}\right)/3 =$ (28,57 – 14,29 + 57,14 – 42,86 + 85,71 – 71,43)/3 = 14,29, $l^{(5)} = l_1^{(5)} + l_2^{(5)} =$ 14,29 + 14,29 = 28,58.

2-кезең. (2.24) көмегімен кеңейуші төбенің номерін анықтауды жүзеге асыру үшін яғни:

$$s = j \text{ егер } \left(x_j \le k_1^{(m+1)} \le x_{j+1}\right) \text{немесе} \left(x_j \ge k_1^{(m+1)} \ge x_{j+1}\right), \qquad (2.24)$$

мұндағы $k_1^{(m+1)}$ - (2.22) арқылы анықталатын түзетуші параметр.

бірінші итерация - $x_1 = b_{21}^{(3)} - b_{11}^{(3)} =$ 20 – 0 = 20, $x_2 = b_{22}^{(3)} - b_{12}^{(3)}$ = 60 – 40=20, $x_3 = b_{23}^{(3)} - b_{13}^{(3)}$ = 100 –80 = 20. Көрініп тұрғандай кезінде $\left(x_1 \le k_1^{(4)} \le x_2\right)$ => (20 ≤ 20 ≤ 20) s=1 болады, кезінде $\left(x_2 \le k_1^{(4)} \le x_3\right)$ => (20 ≤ 20 ≤ 20) s=2 болады т.б. НЕС таралуы бірқалыпты болғандықтан, кеңейтуші төбелер бірнешеу болады да, осылай, s түрінде кез келген j ($j = \overline{1,3}$) қолдануға болады. Осыдан шыға отырып, мысалы, қосымша термді құруды бірінші төбеден кейін жүзеге асырамыз яғни бірінші және екінші $\underset{\sim}{T}_{LR}^{(3)}$ термдер арасында;

екінші итерация - $x_1 = b_{21}^{(4)} - b_{11}^{(4)} =$ 14,29 – 0 = 14,29, $x_2 = b_{22}^{(4)} - b_{12}^{(4)}$ = 42,86 – 28,57=14,29, $x_3 = b_{23}^{(4)} - b_{13}^{(4)}$ = 71,43 –57,14 = 14,29, $x_4 = b_{24}^{(4)} - b_{14}^{(4)}$ = 100,0 – 85,71 = 14,29. Көрініп тұрғандай $\left(x_1 \le k_1^{(5)} \le x_2\right)$ => (14,29 ≤ 14,29 ≤ 14,29) кезінде s=1, $\left(x_2 \le k_1^{(5)} \le x_3\right)$ => (14,29 ≤ 14,29 ≤14,29) кезінде s=2 т.б. Бірінші итерацияға ұқсастығы бойынша s түрінде j ($j = \overline{1,4}$) кез келгенін қолдануға болады. Осыдан шыға отырып, мысалы, қосымша термді орнатуды бірінші төбеден кейін жүзеге асырамыз яғни бірінші және екінші $\underset{\sim}{T}_{LR}^{(4)}$ терм аралығында .

3- Кезең. (2.25) және (2.26) формулаларына сәйкес трапецияның жоғарғы және төменгі ірге абсцисінің мәнін шығару яғни.:

$$b_{1j}^{(m+1)'} = \begin{cases} b_{1j}^{(m)} \text{ егер } j < s+1; \\ b_{2\,j-1}^{(m)} + k_2^{(m+1)} \text{ егер } j = s+1; \\ b_{1j-1}^{(m)} + k^{(m+1)} \text{ егер } j > s+1, \end{cases} \quad b_{2j}^{(m+1)'} = \begin{cases} b_{2j}^{(m)} \text{ егер } j < s+1; \\ b_{1j}^{(m+1)'} + k_1^{(m+1)} \text{ егер } j = s+1; \\ b_{2j-1}^{(m)} + k^{(m+1)} \text{ егер } j > s+1, \end{cases} \quad j = \overline{1,m}, \qquad (2.25)$$

$$a_j^{(m+1)'} = \begin{cases} a_j^{(m)} \text{ егер } j < s+2; \\ c_{j-2}^{(m+1)'} + l_1^{(m+1)} \text{ егер } j = s+2; \\ a_{j-1}^{(m)} + l^{(m+1)} \text{ егер } j > s+2, \end{cases} \quad c_j^{(m+1)'} = \begin{cases} c_j^{(m)} \text{ егер } j < s \\ a_{j+1}^{(m)} + l_2^{(m+1)} \text{ егер } j = s; \\ c_{j-1}^{(m)} + l^{(m+1)} \text{ егер } j > s, \end{cases} \quad j = \overline{1,m}, \qquad (2.26)$$

мұндағы m – бастапқы терм-жиынтық саны.

бірінші итерация - 1 < 2 егер $b_{11}^{(4)\prime} = b_{11}^{(3)}$ = 0, 1 < 2 егер $b_{21}^{(4)\prime} = b_{21}^{(3)}$ = 20, 2 = 2 егер $b_{12}^{(4)\prime} = b_{21}^{(3)} + k_2^{(4)}$ = 20 + 20 = 40, 2 = 2 егер $b_{22}^{(4)\prime} = b_{12}^{(4)\prime} + k_1^{(4)}$ = 40 + 20 = 60, 3 > 2 егер $b_{13}^{(4)\prime} = b_{12}^{(3)} + k^{(4)}$ = 40 + 40 = 80, 4 > 2 егер $b_{23}^{(4)\prime} = b_{22}^{(3)} + k^{(4)}$ = 60 + 40 = 100 3 > 2, $b_{14}^{(4)\prime} = b_{13}^{(3)} + k^{(4)}$ = 80 + 40 = 120, 4 > 2 егер $b_{24}^{(4)\prime} = b_{23}^{(3)} + k^{(4)}$ = 100 + 40 = 140.

Ұқсас түрде төменгі абсцистердің іргесін есептейік, яғни: 1 < 3 кезінде $a_1^{(4)\prime} = a_1^{(3)}$ = 0, 2 < 3 егер $a_2^{(4)\prime} = a_2^{(3)}$ = 20, 1 = 1 егер $c_1^{(4)\prime} = a_2^{(3)} + l_2^{(4)}$ = 20 + 20 = 40, 3 = 3 егер $a_3^{(4)\prime} = c_1^{(4)\prime} + l_1^{(4)}$ = 40 + 20 = 60 , 2 > 1 егер $c_2^{(4)\prime} = c_1^{(3)} + l^{(4)}$ = 40 + 20 = 60, 4 > 3 егер $a_4^{(4)\prime} = a_3^{(3)} + l^{(4)}$ = 60 + 40 = 100, 3 > 1 егер $c_3^{(4)\prime} = c_2^{(3)} + l^{(4)}$ = 80 + 40 = 120, 4 > 1 егер $c_4^{(4)\prime} = c_3^{(3)} + l^{(4)}$ = 100 + 40 = 140;

екінші итерация - 1 < 2 егер $b_{11}^{(5)\prime} = b_{11}^{(4)}$ = 0, 1 < 2 егер $b_{21}^{(5)\prime} = b_{21}^{(4)}$ = 14,29, 2 = 2 егер $b_{12}^{(5)\prime} = b_{21}^{(4)} + k_2^{(5)}$ = 14,29 + 14,29 = 28,58, 2 = 2 егер $b_{22}^{(5)\prime} = b_{12}^{(5)\prime} + k_1^{(5)}$ = 28,58 + 14,29 = 42,87, 3 > 2 егер $b_{13}^{(5)\prime} = b_{12}^{(4)} + k^{(5)}$ = 28,58 + 28,58 = 57,16, 3 > 2 $b_{23}^{(5)\prime} = b_{22}^{(4)} + k^{(5)}$ = 42,87 + 28,58 = 71,45 , 4 > 2 егер $b_{14}^{(5)\prime} = b_{13}^{(4)} + k^{(5)}$ = 57,16 + 28,58 = 85,74, 4 > 2 егер $b_{24}^{(5)\prime} = b_{23}^{(4)} + k^{(5)}$ = 71,45 + 28,58 = 100,03, 5 > 2 егер $b_{15}^{(5)\prime} = b_{14}^{(4)} + k^{(5)}$ = 85,74 + 28,55 = 114,32, 5 > 2 егер $b_{25}^{(5)\prime} = b_{24}^{(4)} + k^{(5)}$ = 100,03 + 28,58 = 128,61.

Ұқсас түрде төменгі абсцистердің іргесін есептейік яғни.: 1 < 3 егер $a_1^{(5)\prime} = a_1^{(4)}$ = 0, 2 < 3 егер $a_2^{(5)\prime} = a_2^{(4)}$ = 14,285, 1 = 1 егер $c_1^{(5)\prime} = a_2^{(4)} + l_2^{(5)}$ = 14,285 + 14,285 = 28,57, 3 = 3 егер $a_3^{(5)\prime} = c_1^{(4)} + l_1^{(5)}$ = 28,57 + 14,29 = 42,86, 2 > 1 егер $c_2^{(5)\prime} = c_1^{(4)} + l^{(5)}$ = 28,57 + 28,57 = 57,14, 4 > 3 егер $a_4^{(5)\prime} = a_3^{(4)} + l^{(5)}$ = 42,86 + 28,57 = 71,43, 3 > 1 егер $c_3^{(5)\prime} = c_2^{(4)} + l^{(5)}$ = 57,14 + 28,57 = 85,71, 5 > 3 егер $a_5^{(5)\prime} = a_4^{(4)} + l^{(5)}$ = 71,43 + 28,57 = 100,0, 4 > 1 егер $c_4^{(5)\prime} = c_3^{(4)} + l^{(5)}$ = 85,71 + 28,57 = 114,29, 5 > 1 егер $c_5^{(5)\prime} = c_4^{(4)} + l^{(5)}$ = 100,00 + 28,57 = 128,57.

4-кезең. (2.27)-(2.30) формулалар көмегімен, екі қадамды бірізділік негізінде (b_{dr} = c_{dr} = 100 кезінде) алынған эталонды мәндердің мөлшерлеуін жүзеге асырайық.

$$k_3^{(m+1)} = \frac{b_{dr}}{b_{2m+1}^{(m+1)\prime}}, \tag{2.27}$$

$$l_3^{(m+1)} = \frac{c_{dr}}{c_{m+1}^{(m+1)\prime}}, \tag{2.28}$$

мұндағы b_{dr} және c_{dr} сәйкесінше трапеция іргесінің жоғарғы және төменгі абсцистерінің максималды мәні.

$$b_{ij}^{(m+1)} = b_{ij}^{(m+1)\prime} \times k_3^{(m+1)},\ i = \overline{1,2},\ j = \overline{1,m}; \tag{2.29}$$

$$a_j^{(m+1)} = a_j^{(m+1)\prime} \times l_3^{(m+1)}, \qquad c_j^{(m+1)} = c_j^{(m+1)\prime} \times l_3^{(m+1)}, \; j = \overline{1,m}. \qquad (2.30)$$

Бірінші итерация:

1-қадам. (2.27) және (2.28) формулалары бойынша коэффициенттер мөлшерін шығару: $k_3^{(4)} = b_{dr} / b_{24}^{(4)\prime} = 100 / 140 = 0{,}71$, $l_3^{(4)} = c_{dr} / c_4^{(4)\prime} = 100 / 140 = 0{,}71$.

2-қадам. 3-кезеңде алынған эталонды мәндерді (2.29) және (2.30) формулалары көмегімен мөлшерлейміз: $b_{11}^{(4)} = b_{11}^{(4)\prime} \times k_3^{(4)} = 0 \times 0{,}71 = 0$, $b_{21}^{(4)} = b_{21}^{(4)\prime} \times k_3^{(4)} = 20 \times 0{,}71 = 14{,}29$, $b_{12}^{(4)} = b_{12}^{(4)\prime} \times k_3^{(4)} = 40 \times 0{,}71 = 28{,}57$, $b_{22}^{(4)} = b_{22}^{(4)\prime} \times k_3^{(4)} = 60 \times 0{,}71 = 42{,}86$, $b_{13}^{(4)} = b_{13}^{(4)\prime} \times k_3^{(4)} = 80 \times 0{,}71 = 57{,}14$, $b_{23}^{(4)} = b_{23}^{(4)\prime} \times k_3^{(4)} = 100 \times 0{,}71 = 71{,}43$, $b_{14}^{(4)} = b_{14}^{(4)\prime} \times k_3^{(4)} = 120 \times 0{,}71 = 85{,}71$, $b_{24}^{(4)} = b_{24}^{(4)\prime} \times k_3^{(4)} = 140 \times 0{,}71 = 100$,

$a_1^{(4)} = a_1^{(4)\prime} \times l_3^{(4)} = 0 \times 0{,}71 = 0$, $a_2^{(4)} = a_2^{(4)\prime} \times l_3^{(4)} = 20 \times 0{,}71 = 14{,}29$, $a_3^{(4)} = a_3^{(4)\prime} \times l_3^{(4)} = 60 \times 0{,}71 = 42{,}86$, $a_4^{(4)} = a_4^{(4)\prime} \times l_3^{(4)} = 100 \times 0{,}71 = 71{,}43$, $c_1^{(4)} = c_1^{(4)\prime} \times l_3^{(4)} = 40 \times 0{,}71 = 28{,}57$, $c_2^{(4)} = c_2^{(4)\prime} \times l_3^{(4)} = 80 \times 0{,}71 = 57{,}14$, $c_3^{(4)} = c_3^{(4)\prime} \times l_3^{(4)} = 120 \times 0{,}71 = 85{,}71$, $c_4^{(4)} = c_4^{(4)\prime} \times l_3^{(4)} = 140 \times 0{,}71 = 100$.

Екінші итерация:

1-қадам. (2.27) және (2.28) формулалары бойынша мөлшерлеуші коэффициенттерді шығарамыз: $k_3^{(5)} = b_{dr} / b_{25}^{(5)\prime} = 100 / 128{,}57 = 0{,}78$, $l_3^{(5)} = c_{dr} / c_5^{(5)\prime} = 100 / 128{,}57 = 0{,}78$.

2-қадам. 3-кезеңде алынған эталонды мәндерді (2.29) және (2.30) формулалары көмегімен мөлшерлейміз: $b_{11}^{(5)} = b_{11}^{(5)\prime} \times k_3^{(5)} = 0 \times 0{,}78 = 0$, $b_{21}^{(5)} = b_{21}^{(5)\prime} \times k_3^{(5)} = 14{,}29 \times 0{,}78 = 11{,}11$, $b_{12}^{(5)} = b_{12}^{(5)\prime} \times k_3^{(5)} = 28{,}57 \times 0{,}78 = 22{,}22$, $b_{22}^{(5)} = b_{22}^{(5)\prime} \times k_3^{(5)} = 42{,}86 \times 0{,}78 = 33{,}33$, $b_{13}^{(5)} = b_{13}^{(5)\prime} \times k_3^{(5)} = 57{,}14 \times 0{,}78 = 44{,}44$, $b_{23}^{(5)} = b_{23}^{(5)\prime} \times k_3^{(5)} = 71{,}43 \times 0{,}78 = 55{,}55$, $b_{14}^{(5)} = b_{14}^{(5)\prime} \times k_3^{(5)} = 85{,}71 \times 0{,}78 = 66{,}66$, $b_{24}^{(5)} = b_{24}^{(5)\prime} \times k_3^{(5)} = 100{,}00 \times 0{,}78 = 77{,}77$, $b_{15}^{(5)} = b_{15}^{(5)\prime} \times k_3^{(5)} = 114{,}29 \times 0{,}78 = 88{,}88$, $b_{25}^{(5)} = b_{25}^{(5)\prime} \times k_3^{(5)} = 128{,}57 \times 0{,}78 = 100$,

$a_1^{(5)} = a_1^{(5)\prime} \times l_3^{(5)} = 0 \times 0{,}78 = 0$, $a_2^{(5)} = a_2^{(5)\prime} \times l_3^{(5)} = 14{,}29 \times 0{,}78 = 11{,}11$, $a_3^{(5)} = a_3^{(5)\prime} \times l_3^{(5)} = 42{,}86 \times 0{,}78 = 33{,}33$, $a_4^{(5)} = a_4^{(5)\prime} \times l_3^{(5)} = 71{,}43 \times 0{,}78 = 55{,}55$, $a_5^{(5)} = a_5^{(5)\prime} \times l_3^{(5)} = 100{,}0 \times 0{,}78 = 77{,}77$, $c_1^{(5)} = c_1^{(5)\prime} \times l_3^{(5)} = 28{,}57 \times 0{,}78 = 22{,}22$, $c_2^{(5)} = c_2^{(5)\prime} \times l_3^{(5)} = 57{,}14 \times 0{,}78 = 44{,}44$, $c_3^{(5)} = c_3^{(5)\prime} \times l_3^{(5)} = 85{,}71 \times 0{,}78 = 66{,}66$, $c_4^{(5)} = c_4^{(5)\prime} \times l_3^{(5)} = 114{,}29 \times 0{,}78 = 88{,}88$, $c_5^{(5)} = c_5^{(5)\prime} \times l_3^{(5)} = 128{,}57 \times 0{,}78 = 100$.

ЛА термдерін трансформациялау нәтижесінде аламыз, мысалы, $\underset{\sim}{T}_{LR}^{(5)}$ үшін (2.20)-нан лингвистикалық мәндер сәйкес келетін эквивалентті сандары және 4-кезеңнің 2-қадамында анықталған олардың мәндері 2.17-кестесіне енгізілген.

Кесте 2.17 - Инкременттелген эталонды трапеция түрдегі НЕС

LR ЛА НЕС таралу типі	НЕС $\underset{\sim}{T}_{LR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ $(j=\overline{1,5})$				
	$\underset{\sim}{T}_{LR_1}$	$\underset{\sim}{T}_{LR_2}$	$\underset{\sim}{T}_{LR_3}$	$\underset{\sim}{T}_{LR_4}$	$\underset{\sim}{T}_{LR_5}$
Бірқалыпты	*(0;0;11,11; 22,22)*$_{LR}$	*(11,11;22,22;33,33; 44,44)*$_{LR}$	*(33,34;44,44;55,55; 66,66)*$_{LR}$	*(55,55;66,66;77,77; 88,88)*$_{LR}$	*(77,77;88,88; 100;100)*$_{LR}$
Бірқалыпты емес	*(0;0;9,97; 19,37)*$_{LR}$	*(9,96;21,59;32,29; 44,83)*$_{LR}$	*(33,21;41,7;55,54; 67,16)*$_{LR}$	*(55,54;67,16;77,86; 91,7)*$_{LR}$	*(77,86;91,7; 100;100)*$_{LR}$
Өсуші	*(0;0;1,65; 8,81)*$_{LR}$	*(1,65;8,81;18,17; 30,55)*$_{LR}$	*(18,17;30,55;40,64; 53,03)*$_{LR}$	*(40,64;53,03;63,12; 80,73)*$_{LR}$	*(63,12;80,73; 100;100)*$_{LR}$
Төмендеуші	*(0;0;15,58; 26,44)*$_{LR}$	*(15,58;26,44;37,76; 48,61)*$_{LR}$	*(37,76;48,61;59,93; 72,73)*$_{LR}$	*(59,93;72,73;83,86; 92,76)*$_{LR}$	*(83,86;92,76; 100;100)*$_{LR}$

Әрі қарай $\underset{\sim}{T}_{LR}^{(5)}$ үшін бірқалыптылық шартын есептейміз: Ω_p =(11,11 - 0 = 33,33 – 22,22) Λ (33,33 – 22,22 = 55,55 – 44,44) Λ (55,55 – 44,44 = 77,77 – 66,66) Λ (77,77 – 66,66 = 100 – 88,88) Λ (22,22 – 11,11 = 44,44 – 33,33) Λ (44,44 – 33,33 = 66,66 - 55,55) Λ (66,66 - 55,55 = 88,88 -77,77) = 1.

Көріп тұрғанымыздай $\underset{\sim}{T}_{LR}^{(5)}$ мен $\underset{\sim}{T}_{LR}^{(3)}$ сияқты $\Omega_p = 1$ ие, бұл орындалған қайта жаңғыртулардың эквиваленттігі туралы айтып отыр. Бастапқы және қайта жаңғырған эталондардың $\underset{\sim}{T}_{LR}^{(3)}$ және $\underset{\sim}{T}_{LR}^{(5)}$ НЕС-на бірқалыпты таралуының графикалық түсіндірілуі 2.3-суретте (*а, б*) берілген.

2-үлгі – бірқалыпты емес таралу типі. 1-үлгідегі сияқты ЛА $\boldsymbol{LR}^{(3)}$ (2.19) формуласындағы термдермен анықталған болсын. НЕС-ң *lr* осі, олардың сандық $\underset{\sim}{T}_{LR_j}$, $j=\overline{1,3}$ эквиваленттер бойынша 2.16-кестеде бірқалыпты таралмаған үлгіде әдіс жұмысын қарастырайық яғни олар үшін бірқалыпты емес шарттылық шындық болады: $\Omega_н = (b_{21} - b_{11} \neq b_{22} - b_{12}) \vee (b_{22} - b_{12} \neq b_{23} - b_{13}) + (b_{12} - b_{21} \neq b_{13} - b_{22}) = (18 – 0 \neq 60 – 35) \vee (60 – 35 \neq 100 – 85) + (35 – 18 \neq 85 – 60) = 1 \vee 1 + 1 = 1$. Көріп тұрғанымыздай бірқалыпты еместік шарттылықтары шын ($\Omega_н$=1). Бұл $\boldsymbol{LR}^{(3)}$ ЛА НЕС -ның бірқалыпты емес таралу типіне сәйкес келеді.

1-4 кезеңдерге сәйкес (2.18) формуласы бойынша ЛА $\boldsymbol{LR}^{(3)}$ n-еселі инкременттеу орындалады.

1-кезең. (2.22) және (2.23) формулалары бойынша түзетуші параметрлерді іздеуді жүзеге асырамыз яғни.:

Бірінші итерация - $k_1^{(4)} = 19{,}33$, $k_2^{(4)} = 21$, $k^{(4)} = 40{,}33$, $l_1^{(4)} = 19{,}33$, $l_2^{(4)} = 21$, $l^{(4)} = 40{,}33$;

Екінші итерация - $k_1^{(5)} = 13{,}78$, $k_2^{(5)} = 14{,}96$, $k^{(5)} = 28{,}74$, $l_1^{(5)} = 13{,}78$, $l_2^{(5)} = 14{,}94$, $l^{(5)} = 28{,}74$.

2-кезең. Мұнда (2.24) формуласы бойынша кеңейуші төбенің номерін анықтау жүзеге асырылады яғни.:

Бірінші итерация - $x_1 = 18$, $x_2 = 25$, $x_3 = 15$, онда $\left(x_2 \geq k_1^{(4)} \geq x_3\right)$ =>(25≥19,33≥15) кезінде s=2. Бұл үлгіде қосымша термді орнатуды екінші төбеден кейін жүзеге асырамыз яғни бірінші және екінші термдер арасында $T_{\underset{\sim}{LR}}^{(3)}$

Екінші итерация - $x_1 = 12{,}83$, $x_2 = 17{,}81$, $x_3 = 13{,}78$, $x_4 = 10{,}69$, онда $\left(x_1 \leq k_1^{(5)} \leq x_2\right)$=>(12,83≤13,78≤17,81) кезінде s=1. Бұл үлгіде қосымша термді орнатуды бірінші төбеден кейін жүзеге асырамыз яғни бірінші және екінші термдер арасында $T_{\underset{\sim}{LR}}^{(4)}$.

3-кезең. (2.25) және (2.26) формулаларының көмегімен трапеция іргелерінің жоғары және төмен абсцисс мәндерін есептеуді жүргіземіз яғни.:

бірінші итерация - $b_{11}^{(4)\prime} = b_{11}^{(3)} = 0$, $b_{21}^{(4)\prime} = b_{21}^{(3)} = 18$, $b_{12}^{(4)\prime} = b_{12}^{(3)} = 35$, $b_{22}^{(4)\prime} = b_{22}^{(3)} = 60$, $b_{13}^{(4)\prime} = b_{22}^{(3)} + k_2^{(4)} = 81$, $b_{23}^{(4)\prime} = b_{13}^{(4)\prime} + k_1^{(4)} = 100{,}33$, $b_{14}^{(4)\prime} = b_{13}^{(3)} + k^{(4)} = 125{,}33$, $b_{24}^{(4)\prime} = b_{23}^{(3)} + k^{(4)} = 140{,}33$,

$a_1^{(4)\prime} = a_1^{(3)} = 0$, $a_2^{(4)\prime} = a_2^{(3)} = 18$, $a_3^{(4)\prime} = a_3^{(3)} = 60$, $a_4^{(4)\prime} = c_2^{(4)\prime} + l_1^{(4)} = 100{,}33$, $c_1^{(4)\prime} = c_1^{(3)} = 35$, $c_2^{(4)\prime} = a_3^{(3)} + l_2^{(4)} = 81$, $c_3^{(4)\prime} = c_2^{(3)} + l^{(4)} = 125{,}33$, $c_4^{(4)\prime} = c_3^{(3)} + l^{(4)} = 140{,}33$;

екінші итерация - $b_{11}^{(5)\prime} = b_{11}^{(4)} = 0$, $b_{21}^{(5)\prime} = b_{21}^{(4)} = 12{,}83$, $b_{12}^{(5)\prime} = b_{12}^{(4)} = 27{,}79$, $b_{22}^{(5)\prime} = b_{22}^{(4)} = 41{,}57$, $b_{13}^{(5)\prime} = b_{22}^{(4)} + k_2^{(5)} = 53{,}68$, $b_{23}^{(5)\prime} = b_{13}^{(5)\prime} + k_1^{(5)} = 71{,}50$, $b_{14}^{(5)\prime} = b_{13}^{(4)} + k^{(5)} = 86{,}46$, $b_{24}^{(5)\prime} = b_{23}^{(4)} + k^{(5)} = 100{,}24$, $b_{15}^{(5)\prime} = b_{14}^{(4)} + k^{(5)} = 118{,}05$, $b_{25}^{(5)\prime} = b_{24}^{(4)} + k^{(5)} = 128{,}74$,

$a_1^{(5)\prime} = a_1^{(4)} = 0$, $a_2^{(5)\prime} = a_2^{(4)} = 12{,}83$, $a_3^{(5)\prime} = a_3^{(4)} = 42{,}76$, $a_4^{(5)\prime} = c_2^{(5)\prime} + l_1^{(5)} = 71{,}50$, $a_5^{(5)\prime} = a_4^{(4)} + l^{(5)} = 100{,}24$, $c_1^{(5)\prime} = c_1^{(4)} = 24{,}94$, $c_2^{(5)\prime} = a_3^{(4)} + l_2^{(5)} = 57{,}72$, $c_3^{(5)\prime} = c_2^{(4)} + l^{(5)} = 86{,}46$, $c_4^{(5)\prime} = c_3^{(4)} + l^{(5)} = 118{,}05$,. $c_5^{(5)\prime} = c_4^{(4)} + l^{(5)} = 128{,}74$.

4-кезең. (2.27) - (2.30) формулаларының көмегімен 2 қадамда алынған мәндер мөлшерін жүзеге асырамыз**.**

1-қадам. (2.27) және (2.28) формулалары бойынша мөлшерлеуші коэффициенттерді табамыз:

бірінші итерация - $k_3^{(4)} = 0{,}71$, $l_3^{(4)} = 0{,}71$;

екінші итерация - $k_3^{(5)} = 0{,}78$, $l_3^{(5)} = 0{,}78$.

2-қадам. (2.29) және (2.30) формулаларына байланысты алынған эталондарды мөлшерлеудің жүзеге асуы яғни.:

бірінші итерация - $b_{11}^{(4)} = 0$, $b_{21}^{(4)} = 12{,}83$, $b_{12}^{(4)} = 24{,}94$, $b_{22}^{(4)} = 42{,}76$, $b_{13}^{(4)} = 57{,}72$, $b_{23}^{(4)} = 71{,}5$, $b_{14}^{(4)} = 89{,}31$, $b_{24}^{(4)} = 100$,

$a_1^{(4)} = 0$, $a_2^{(4)} = 12{,}83$, $a_3^{(4)} = 42{,}76$, $a_4^{(4)} = 71{,}5$, $c_1^{(4)} = 24{,}94$, $c_2^{(4)} = 57{,}72$, $c_3^{(4)} = 89{,}31$, $c_4^{(4)} = 100$,

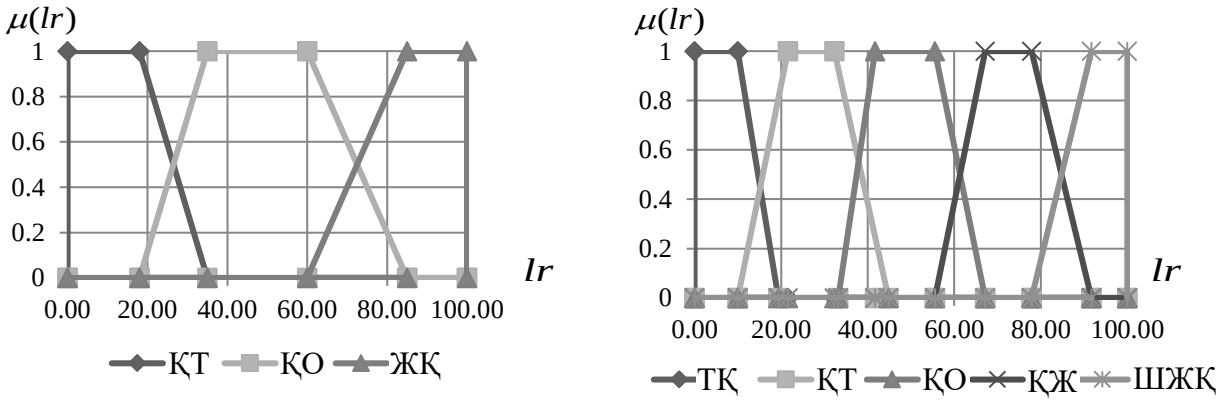
екінші итерация - $b_{11}^{(5)} = 0$, $b_{21}^{(5)} = 9{,}96$, $b_{12}^{(5)} = 21{,}59$, $b_{22}^{(5)} = 32{,}29$, $b_{13}^{(5)} = 41{,}7$, $b_{23}^{(5)} = 55{,}54$, $b_{14}^{(5)} = 67{,}16$, $b_{24}^{(5)} = 77{,}86$, $b_{15}^{(5)} = 91{,}7$, $b_{25}^{(5)} = 100$,

$a_1^{(5)} = 0$, $a_2^{(5)} = 9{,}96$, $a_3^{(5)} = 33{,}21$, $a_4^{(5)} = 55{,}54$, $a_5^{(5)} = 77{,}86$, $c_1^{(5)} = 19{,}37$, $c_2^{(5)} = 44{,}83$, $c_3^{(5)} = 67{,}16$, $c_4^{(5)} = 91{,}7$, $c_5^{(5)} = 100$.

Бір еселі инкременттеу нәтижесінде, мысалы $\underset{\sim}{T}_{LR}^{(5)}$ үшін (2.20) термдер мәнін аламыз, ал оның эквивалент сандарынын 2.17-кестесінде береміз.

Жүргізілген жаңғыртулардан кейін $\underset{\sim}{T}_{LR}^{(5)}$ үшін $\Omega_н$ есептейік: $\Omega_н = (9{,}96 - 0 \neq 32{,}29 - 21{,}59) \vee (32{,}29 - 21{,}59 \neq 55{,}54 - 41{,}7) \vee (55{,}54 - 41{,}7 \neq 77{,}86 - 67{,}16) \vee (77{,}86 - 67{,}16 \neq 100 - 91{,}7) + (21{,}59 - 9{,}96 \neq 41{,}7 - 32{,}29) \vee (41{,}7 - 32{,}29 \neq 67{,}16 - 55{,}54) \vee (67{,}16 - 55{,}54 \neq 91{,}7 - 100) = 1$. $\underset{\sim}{T}_{LR}^{(5)}$ бірқалыпты емес шарттылық $\underset{\sim}{T}_{LR}^{(3)}$ сияқты $\Omega_н = 1$ шындық болып табылады, бұл орындалған қайта жаңғыртулардың эквиваленттігі туралы айтады.

НЕС бірқалыпты емес таралуының бастапқы және қайта жаңғырған эталондарының графикалық түсіндірілуі $\underset{\sim}{T}_{LR}^{(3)}$ және $\underset{\sim}{T}_{LR}^{(5)}$ 2.4 (*а, б*)-суретінде берілген.



а) б)

Сурет 2.4 - ***LR*** ЛА үшін НЕС бірқалыпты емес таралуының этолонды мәндерінің термдері

а) $\underset{\sim}{T}^{(3)}_{LR}$; б) $\underset{\sim}{T}^{(5)}_{LR}$

3-үлгі – таралудың өсу типі. (2.19)-дан термдермен $\boldsymbol{LR}^{(3)}$ ЛА үшін берілген әдістің жұмысын көрсетейік, 2.16-кестесінен $\underset{\sim}{T}_{LR_j}$, $j=\overline{1,3}$ олардың

сандық мәні *lr* осіне қарай таралудың өсу типіне ие, демек өсу шарттылығы ол үшін шындық болып табылады: $\Omega_в$ =(b_{21} - b_{11} < b_{22} - b_{12}) Λ (b_{22} - b_{12} < b_{23} - b_{13}) Λ (b_{12} - b_{21} < b_{13} - b_{22}) = (3 - 0 < 33 – 15,48) Λ (33 – 16 < 100 – 65) Λ (16– 3 < 100 – 65) = 1 Λ 1 Λ 1 = 1. Көрініп тұрғандай, $\Omega_в=1$ шарттылық шындық, бұл $\boldsymbol{LR}^{(3)}$ ЛА НЕС-ң таралудың өсу типіне сәйкес келуін айтады.

НЕС бірқалыпты таралуына арналған үлгіге ұқсас 1-4 кезеңдерге сәйкес келетін қайта жаңғыртулар жүргіземіз (2.18).

1-кезең. (2.22) және (2.23) мәндері бойынша түзетуші параметрлерді іздеуді жүзеге асырайық, демек:

Бірінші итерация- $k_1^{(4)}=18{,}33$, $k_2^{(4)}=22{,}5$, $k^{(4)}=40{,}83$, $l_1^{(4)}=18{,}33$, $l_2^{(4)}=22{,}5$, $l^{(4)}=40{,}83$;

Екінші итерация - $k_1^{(5)}=13{,}02$, $k_2^{(5)}=15{,}98$, $k^{(5)}=28{,}99$, $l_1^{(5)}=13{,}02$, $l_2^{(5)}=15{,}98$, $l^{(5)}=28{,}99$.

2-кезең. Енді (2.24) формуласы бойынша кеңейуші төбенің номерін анықтайық.

бірінші итерация - $x_1=3$, $x_2=17$, $x_3=35$ болса, онда $\left(x_2 \le k_1^{(4)} \le x_3\right)$ => (17 ≤ 18,33 ≤ 35) кезінде s=2 болады. Мұнда қосымша термді құруды екінші төбеден кейін яғни $\underset{\sim}{T}^{(3)}_{LR}$ екінші және үшінші термдерден кейін жүзеге асырамыз;

екінші итерация - $x_1=2{,}13$, $x_2=12{,}07$, $x_3=13{,}02$, $x_4=24{,}85$ болса, онда $\left(x_2 \le k_1^{(5)} \le x_3\right)$ => (12,07 ≤ 13,02 ≤ 13,02) кезінде s=2 болады. Мұнда қосымша термді құруды екінші төбеден кейін яғни $\underset{\sim}{T}^{(4)}_{LR}$ екінші және үшінші термдерден кейін жүзеге асырамыз;

3-кезең. (2.25) және (2.26) формулалар көмегімен трапеция іргесінің жоғарғы және төменгі абсцисс мәндерін есептеуді жүзеге асырамыз, демек:

бірінші итерация - $b_{11}^{(4)\prime}=0$, $b_{21}^{(4)\prime}=3$, $b_{12}^{(4)\prime}=16$, $b_{22}^{(4)\prime}=33$, $b_{13}^{(4)\prime}=55{,}5$, $b_{23}^{(4)\prime}=73{,}83$, $b_{14}^{(4)\prime}=105{,}83$, $b_{24}^{(4)\prime}=140{,}83$,

$a_1^{(4)\prime}=0$, $a_2^{(4)\prime}=3$, $a_3^{(4)\prime}=33$, $a_4^{(4)\prime}=73{,}83$, $c_1^{(4)\prime}=16$, $c_2^{(4)\prime}=55{,}5$, $c_3^{(4)\prime}=105{,}83$, $c_4^{(4)\prime}=140{,}83$;

екінші итерация - $b_{11}^{(5)\prime}=0$, $b_{21}^{(5)\prime}=2{,}13$, $b_{12}^{(5)\prime}=11{,}36$, $b_{22}^{(5)\prime}=23{,}43$, $b_{13}^{(5)\prime}=39{,}41$, $b_{23}^{(5)\prime}=52{,}43$, $b_{14}^{(5)\prime}=68{,}4$, $b_{24}^{(5)\prime}=81{,}42$, $b_{15}^{(5)\prime}=104{,}14$, $b_{25}^{(5)\prime}=128{,}99$,

$a_1^{(5)'} = 0$, $a_2^{(5)'} = 2{,}13$, $a_3^{(5)'} = 23{,}43$, $a_4^{(5)'} = 52{,}43$, $a_5^{(5)'} = 81{,}42$, $c_1^{(5)'} = 11{,}36$, $c_2^{(5)'} = 39{,}41$, $c_3^{(5)'} = 68{,}4$, $c_4^{(5)'} = 104{,}14$,. $c_5^{(5)'} = 128{,}99$.

4-кезең. Әрі қарай алынған нәтижені екі қадаммен (2.27) - (2.30) формулалар көмегімен нормалаймыз**.**

1-Қадам. Нормалаушы коэффициенттерді есептейміз ((2.27) мен (2.28) қара):

бірінші итерация - $k_3^{(4)} = 0{,}71$, $l_3^{(4)} = 0{,}71$;

екінші итерация - $k_3^{(5)} = 0{,}78$, $l_3^{(5)} = 0{,}78$.

2-Қадам. 3-кезеңде алған эталондарды нормалаймыз ((2.29) мен (2.30)қара):

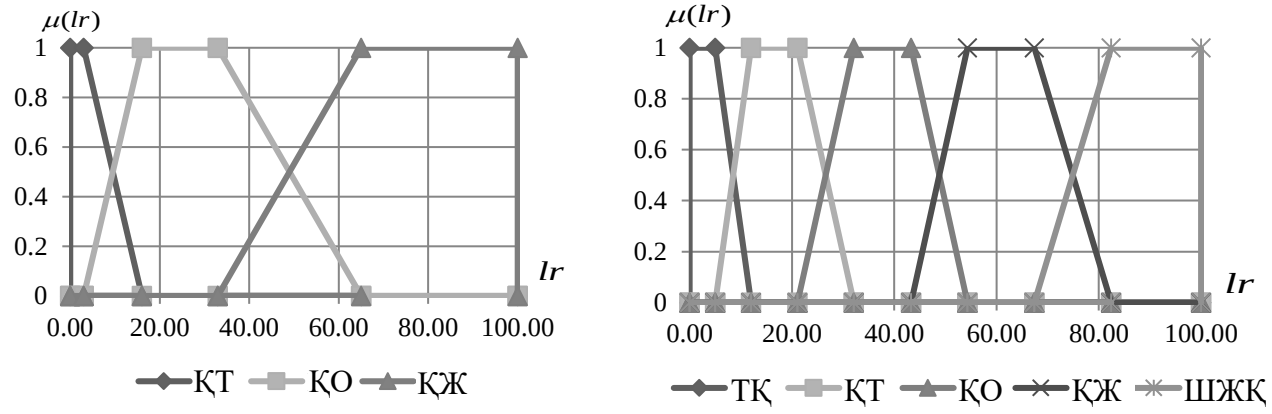
бірінші итерация - $b_{11}^{(4)} = 0$, $b_{21}^{(4)} = 2{,}13$, $b_{12}^{(4)} = 11{,}36$, $b_{22}^{(4)} = 23{,}43$, $b_{13}^{(4)} = 39{,}41$, $b_{23}^{(4)} = 52{,}43$, $b_{14}^{(4)} = 75{,}15$, $b_{24}^{(4)} = 100$,

$a_1^{(4)} = 0$, $a_2^{(4)} = 2{,}13$, $a_3^{(4)} = 23{,}43$, $a_4^{(4)} = 52{,}43$, $c_1^{(4)} = 11{,}36$, $c_2^{(4)} = 39{,}41$, $c_3^{(4)} = 75{,}15$, $c_4^{(4)} = 100$;

екінші итерация - $b_{11}^{(5)} = 0$, $b_{21}^{(5)} = 1{,}65$, $b_{12}^{(5)} = 8{,}81$, $b_{22}^{(5)} = 18{,}17$, $b_{13}^{(5)} = 30{,}55$, $b_{23}^{(5)} = 40{,}64$, $b_{14}^{(5)} = 53{,}03$, $b_{24}^{(5)} = 63{,}12$, $b_{15}^{(5)} = 80{,}73$, $b_{25}^{(5)} = 100$,

$a_1^{(5)} = 0$, $a_2^{(5)} = 1{,}65$, $a_3^{(5)} = 18{,}17$, $a_4^{(5)} = 40{,}64$, $a_5^{(5)} = 63{,}12$, $c_1^{(5)} = 8{,}81$, $c_2^{(5)} = 30{,}55$, $c_3^{(5)} = 53{,}03$, $c_4^{(5)} = 80{,}73$, $c_5^{(5)} = 100$.

$\underset{\sim}{T}_{LR}^{(5)}$ үшін ((2.20) қара) терм мәндерін аламыз, олардың эквиваленттік саны 2.17-кестесіне енгізілген (*сурет* 2.5 *а, б*).



а) б)

Сурет 2.5 - ***LR*** ЛА үшін НЕС таралуының өсу типімен эталон мәнді термдері: а) $\underset{\sim}{T}_{LR}^{(3)}$; б) $\underset{\sim}{T}_{LR}^{(5)}$

Әрі қарай $\underset{\sim}{T}_{LR}^{(5)}$ үшін өсу шарттылығын қарастырайық. n-еселі инкременттеу процесі қосымша термдер қосылуын және олардың сарапшылар талқылауында қалыптасуын тұспалдайды, сондықтан қосымша термдердің мәндері сәйкес келуі мүмкін, демек өсу шарттылығының жеке жағдайын қалыптастыру қажет

яғни: $\Omega_в = \bigwedge_{j=1}^{m-1}(b_{2j}\text{-}b_{1j} \le b_{2j+1}\text{-}b_{1j+1}) \bigwedge_{j=1}^{m-2}(b_{1j+1}\text{-}b_{2j} \le b_{1j+2}\text{-}b_{2j+1})$ болса, демек $\Omega_в = (b_{21} - b_{11} \le b_{22} - b_{12}) \Lambda (b_{22} - b_{12} \le b_{23} - b_{13}) \Lambda (b_{23} - b_{13} \le b_{24} - b_{14}) \Lambda (b_{24} - b_{14} \le b_{25} - b_{15}) \Lambda (b_{12} - b_{21} \le b_{13} - b_{22}) \Lambda (b_{13} - b_{22} \le b_{14} - b_{23}) \Lambda (b_{14} - b_{23} \le b_{15} - b_{24})$ = (1,65 - 0 ≤ 18,17 – 8,81) Λ (18,17 – 8,81 ≤ 40,64 – 30,55) Λ (40,64 – 30,55 ≤ 63,12 – 53,03) Λ (63,12 – 53,03 ≤ 100 – 80,73) Λ (8,81 – 1,65 ≤ 30,55 – 18,17) Λ (30,55 – 18,17 ≤ 53,03 – 40,64) Λ (53,03 – 40,64 ≤ 80,73 –63,12) = 1 Λ 1 Λ 1 Λ 1 Λ 1 Λ 1 Λ 1 = 1 үшін $\underset{\sim}{T}_{LR}^{(5)}$.

Көріп тұрғанымыздай, $\underset{\sim}{T}_{LR}^{(5)}$. үшін $\Omega_в = 1$ мәндері шындық болып табылады, бұл орындалып жатқан жаңғыртулардың адекваттығы туралы деген сөз.

4-үлгі – азаймалы таралу типі. (2.19)-ғы мәнді 2.16-кестесіндегі эквивалент санымен бірге қабылдайтын $\boldsymbol{LR}^{(3)}$ ЛА НЕС-ды трансформациалауды жүзеге асырайық, олар *lr* осінде мынадай азаймалы таралу типіне ие яғни оларға азаю шарттылығы шындық болып табылады, демек: $\Omega_y = (b_{21} - b_{11} > b_{22} - b_{12}) \Lambda (b_{22} - b_{12} > b_{23} - b_{13}) \Lambda (b_{12} - b_{21} > b_{13} - b_{22})$ = (28 - 0 > 71 – 51) Λ (71 – 51 > 100 – 87) Λ (51 – 28 > 87 – 71) = 1 Λ 1 Λ 1 = 1. Көріп тұрғанымыздай, $\Omega_y = 1$, демек $\boldsymbol{LR}^{(3)}$ ЛА НЕС азаймалы таралу типіне сәйкес келеді.

1-4 кезеңдерімен $\boldsymbol{LR}^{(3)}$ ЛА (2.12) n-еселі инкременттеуді сәйкестендіруді жүзеге асыру.

1-кезең. (2.22) мен (2.23) формулалары бойынша түзетуші параметрлерді анықтау, демек:

бірінші итерация - $k_1^{(4)} = 20{,}33$, $k_2^{(4)} = 19{,}5$, $k^{(4)} = 39{,}83$, $l_1^{(4)} = 20{,}33$, $l_2^{(4)} = 19{,}5$, $l^{(4)} = 39{,}83$;

екінші итерация - $k_1^{(5)} = 14{,}54$, $k_2^{(5)} = 13{,}95$, $k^{(5)} = 28{,}49$, $l_1^{(5)} = 14{,}54$, $l_2^{(5)} = 13{,}95$, $l^{(5)} = 28{,}49$.

2-кезең. (2.24) формуласы бойынша кеңею төбесінің номерін іздеуді, демек:

бірінші итерация - $x_1 = 28$, $x_2 = 20$, $x_3 = 13$ болса, онда $\left(x_1 \ge k_1^{(4)} \ge x_2\right)$ => (28 ≥ 20,33 ≥ 20) кеінде s=1 болады. Сонымен бірге, бұл үлгіде, бірқалыпты емес таралу типіндегі сияқты қосымша термді орнату бірінші төбеден кейін яғни $\underset{\sim}{T}_{LR}^{(3)}$ бірінші және екінші термдер арасында жүзеге асырылады.;

екінші итерация - $x_1 = 20{,}02$, $x_2 = 14{,}54$, $x_3 = 14{,}3$, $x_4 = 9{,}3$ болса, онда $\left(x_1 \ge k_1^{(5)} \ge x_2\right)$ => (20,02 ≥ 14,54 ≥ 14,54) кезінде s=1 болады. Мұнда қосымша термді орнатуды бірінші төбеден кейін яғни $\underset{\sim}{T}_{LR}^{(4)}$ бірінші және екінші термдерден кейін жүзеге асырамыз;

3-кезең. (2.25) және (2.26) формулалары көмегімен трапеция іргесінің төменгі және жоғарғы абсцистік мәнін есептеу, демек:

бірінші итерация - $b_{11}^{(4)\prime} = 0$, $b_{21}^{(4)\prime} = 28$, $b_{12}^{(4)\prime} = 47{,}57$, $b_{22}^{(4)\prime} = 67{,}83$, $b_{13}^{(4)\prime} = 90{,}83$, $b_{23}^{(4)\prime} = 110{,}83$, $b_{14}^{(4)\prime} = 126{,}83$, $b_{24}^{(4)\prime} = 139{,}83$,

$a_1^{(4)\prime} = 0$, $a_2^{(4)\prime} = 28$, $a_3^{(4)\prime} = 67{,}83$, $a_4^{(4)\prime} = 110{,}83$, $c_1^{(4)\prime} = 47{,}5$, $c_2^{(4)\prime} = 90{,}83$, $c_3^{(4)\prime} = 126{,}83$, $c_4^{(4)\prime} = 139{,}83$;

екінші итерация - $b_{11}^{(5)\prime} = 0$, $b_{21}^{(5)\prime} = 20{,}02$, $b_{12}^{(5)\prime} = 33{,}97$, $b_{22}^{(5)\prime} = 48{,}51$, $b_{13}^{(5)\prime} = 62{,}46$, $b_{23}^{(5)\prime} = 77$, $b_{14}^{(5)\prime} = 93{,}44$, $b_{24}^{(5)\prime} = 107{,}75$, $b_{15}^{(5)\prime} = 119{,}19$, $b_{25}^{(5)\prime} = 128{,}49$,

$a_1^{(5)\prime} = 0$, $a_2^{(5)\prime} = 20{,}02$, $a_3^{(5)\prime} = 48{,}51$, $a_4^{(5)\prime} = 77$, $a_5^{(5)\prime} = 107{,}75$, $c_1^{(5)\prime} = 33{,}97$, $c_2^{(5)\prime} = 62{,}46$, $c_3^{(5)\prime} = 93{,}44$, $c_4^{(5)\prime} = 119{,}19$,. $c_5^{(5)\prime} = 128{,}49$.

4-кезең. 2 қадаммен (2.27)-(2.30) фомулалар көмегімен толық алынған нәтижелерді нормалаймыз.

1-қадам. (2.27) және (2.28) формулалары бойынша нормалаушы коэффициенттерді есептейік:

бірінші итерация - $k_3^{(4)} = 0{,}72$, $l_3^{(4)} = 0{,}72$;

екінші итерация - $k_3^{(5)} = 0{,}78$, $l_3^{(5)} = 0{,}78$.

2-қадам. (2.29) мен (2.30) формулалары көмгімен алынған эталондарды нормалаймыз:

бірінші итерация - $b_{11}^{(4)} = 0$, $b_{21}^{(4)} = 20{,}02$, $b_{12}^{(4)} = 33{,}97$, $b_{22}^{(4)} = 48{,}51$, $b_{13}^{(4)} = 64{,}96$, $b_{23}^{(4)} = 79{,}26$, $b_{14}^{(4)} = 90{,}7$, $b_{24}^{(4)} = 100$,

$a_1^{(4)} = 0$, $a_2^{(4)} = 20{,}02$, $a_3^{(4)} = 48{,}51$, $a_4^{(4)} = 79{,}26$, $c_1^{(4)} = 33{,}97$, $c_2^{(4)} = 64{,}96$, $c_3^{(4)} = 90{,}7$, $c_4^{(4)} = 100$;

екінші итерация - $b_{11}^{(5)} = 0$, $b_{21}^{(5)} = 15{,}58$, $b_{12}^{(5)} = 26{,}44$, $b_{22}^{(5)} = 37{,}76$, $b_{13}^{(5)} = 48{,}61$, $b_{23}^{(5)} = 59{,}93$, $b_{14}^{(5)} = 72{,}73$, $b_{24}^{(5)} = 83{,}86$, $b_{15}^{(5)} = 92{,}76$, $b_{25}^{(5)} = 100$,

$a_1^{(5)} = 0$, $a_2^{(5)} = 15{,}58$, $a_3^{(5)} = 37{,}76$, $a_4^{(5)} = 59{,}93$, $a_5^{(5)} = 83{,}86$, $c_1^{(5)} = 26{,}44$, $c_2^{(5)} = 48{,}61$, $c_3^{(5)} = 72{,}73$, $c_4^{(5)} = 92{,}76$, $c_5^{(5)} = 100$.

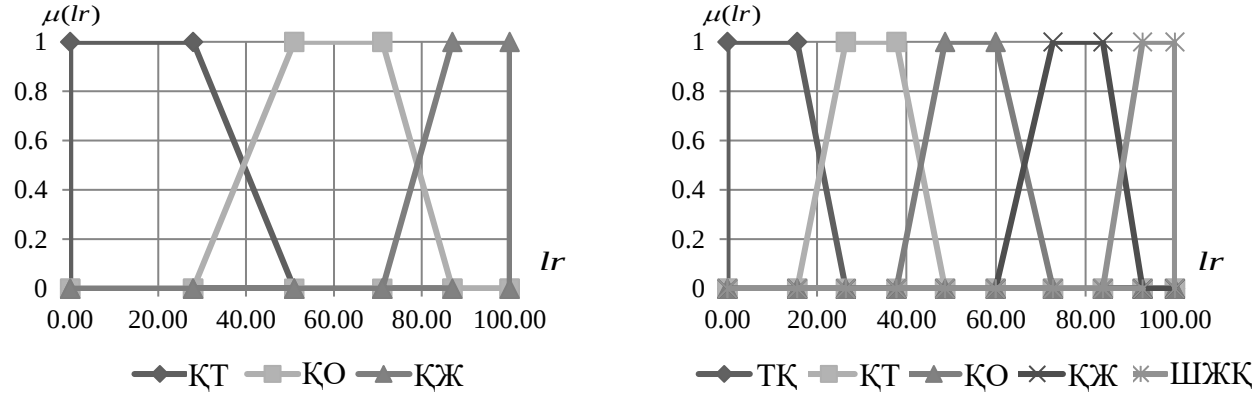
нәтижесінде $\underset{\sim}{T}_{LR}^{(5)}$ үшін ((2.20) қара) термдер мәнін аламыз, оның эквивалентті сандары 2.17-кестесіне енгізілген (2.6 *а* және *б суретін қара*).

$\underset{\sim}{T}_{LR}^{(5)}$ үшін азаймалы шарттылықты тексерейік. Мұнда таралудың өсу типіне ұқсастығы жағынан азаймалы шарттылықтың жеке жағдайын қалыптастыру қажет яғни: $\Omega_y = \bigwedge_{j=1}^{m-1} (b_{2j}\text{-}b_{1j} \geq b_{2j+1}\text{-}b_{1j+1}) \bigwedge_{j=1}^{m-2} (b_{1j+1}\text{-}b_{2j} \geq b_{1j+2}\text{-}b_{2j+1})$ болса, демек $\Omega_y = (b_{21} - b_{11} \geq b_{22} - b_{12}) \Lambda (b_{22} - b_{12} \geq b_{23} - b_{13}) \Lambda (b_{23} - b_{13} \geq b_{24} - b_{14}) \Lambda (b_{24} - b_{14} \geq b_{25} - b_{15}) \Lambda (b_{12} - b_{21} \geq b_{13} - b_{22}) \Lambda (b_{13} - b_{22} \geq b_{14} - b_{23}) \Lambda (b_{14} - b_{23} \geq b_{15} - b_{24}) = (15{,}58 - 0 \geq 37{,}76 - 26{,}44) \Lambda (37{,}76 - 26{,}44 \geq 59{,}93 - 48{,}61) \Lambda (59{,}93 - 48{,}61 \geq 83{,}86 - 72{,}73) \Lambda$

$(83{,}86 - 72{,}73 \geq 100 - 92{,}76) \wedge (26{,}44 - 15{,}58 \geq 48{,}61 - 37{,}76) \wedge (48{,}61 - 37{,}76 \geq 72{,}73 - 59{,}93) \wedge (72{,}73 - 59{,}93 \geq 92{,}76 - 83{,}86) = 1 \wedge 1 \wedge 1 \wedge 1 \wedge 1 \wedge 1 = 1$ үшін $\underset{\sim}{T}_{LR}^{(5)}$.

Көрініп тұрғандай, $\underset{\sim}{T}_{LR}^{(5)}$ үшін және $\underset{\sim}{T}_{LR}^{(3)}$ үшін де $\Omega_y = 1$ мәндер шындық болып табылады да, бұл жаңғыртудың адекваттығы туралы шешім шығаруға мүмкіндік береді.

Міне осылай, ұсынылған ЛА эталондарын трансформациялау қызметін жүзеге асыру әдісі АҚ бар болған қатерлерді бағалау мен анализдеу жүйесінің жұмыс істеу тиімділігін жоғарылатуға мүмкіндік береді. Бұл пәнаралық салаға сарапшыларды қоспай трапециялық түрдегі НЕС-ң термдер санын n-еселі инкременттелуі арқылы жүзеге асады. n-еселі инкременттелуді жасау бұрын құрылған сарапшылар талқылауы негізінде кезінде n термдерін қосу жүзеге асырылады. Міне осылай, n-еселі инкременттеу бір еселі инкременттеуге қарағанда қосымша термдердің қосылуын және олардың қазіргі кезде бар болған сарапшылар талқылауында қалыптасуын тұспалдайды, сондықтан қосымша термдердің мәндері сәйкес келуі мүмкін, демек, азаймалы мен өсу шарттылығын тексеру кезінде шартарға сәйкес жеке жағдайлар құрылған болатын. Термдердің трансформациялану процесін жүзеге асыру бойынша функция мүмкіндіктерін кеңейту үшін бар болған параметриялық НЕС өзге класстарды қолданушы, мысалы үшбұрыш, әдістерді өңдеуді жүзеге асыру қажет.



а) б)

Сурет 2.6 - ***LR*** ЛА үшін НЕС азаймалы таралу типті эталон мәндегі термдер а) $\underset{\sim}{T}_{LR}^{(3)}$; б) $\underset{\sim}{T}_{LR}^{(5)}$

Екінші бөлім бойынша тұжырым

1. Алты компонентті кортежде берілген сипаттама қорының композициясы есебінен сипаттама жиынының динамикалық өзгеруіне қатысты қатерді бағалау мен анализдеу әдісін тиімді, әрі икемдірек құруға мүмкіндік беретін қатер сипаттама қорының кортежді моделі өңделді.

2. Ұсынылған модельді есепке ала отырып, кең спекторлы бар болған ҚБАҚ зерттеу жүргізілді және ҚБАҚ сияқтыларға салыстырмалы анализ жүргізуге болатын және АҚор тапсырмаларын сәйкес түрде шешедегі тиімді

жолды таңдау үшін сипаттама қорының жиыны анықталды.

3. ҚКМ моделі негізінде ҚБАҚ жасауға мүмкіндік беретін әдістер өңделді, бұлар өзге белгілілеріне қарағанда кіріс мәліметтері түрінде сипаттама қорының жиынын қолданып, ол детерминттендірілген, нақты анықталмаған, төмен нысандандырылған ортада функцаланушы жобаланып жатқан бағалау құралдарының кеңею мен икемділігін жоғарылатады .

4. Термдерді бір тәртіпке инкременттеу функциясын n-еселі кеңейтудің модификациясы есебінен сәйкес келетін пән аралық саладағы сарапшылардың қатысуынсыз n тәртіпке ЛА эталонды терм сандарын эквивалентті трансформациялау процесін құру мүмкіндігін кеңейтетін қордың екінші және бірінші жеке кеңейтілуін қолданумен терм сандарын n-еселі инкременттеу функциясын жүзеге асыру әдістері өңделді.

3 АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРІН БАҒАЛАУ ЖҮЙЕСІНІҢ СИНТЕЗІ

3.1 Ақпараттық қауіпсіздік қатерлерін бағалау мен анализдеу жүйесін синтездеу әдістемесі

Әдістемелік негіз ақпаратты қорғау теориясының негізгі құраушысы [85] болып табылады. Ол ақпаратты қорғау ғылыми – зерттеу мәселелерін және беріліп отырған практикалық есепті шешуде қажетті әдістер мен үлгілер жиынтығынан тұрады. Соған байланысты АҚ қатерлерін бағалау және талдау есебінің шешімін табу басты мәселе болып табылады. Мұндай 2.2 тараудағы құралдарды практика жүзінде қолдануда сарапшылар әр уақытта негізгі сипаттамаларды нақты анықтай алмайды, себебі, олар сапалы түрде өрнектеледі. Сол себепті нашар қалыптастырылған, анық емес ортада қатерлерді тиімді бағалау және талдауды сапалы және сандық бағалауларды ескере отырып, жүргізуді жүзеге асыратын жүйелер ерекше көңіл аудартатыны сөзсіз. Осы айтылғандарға байланысты қарастырылып отырған зерттеу жұмысының негізгі мақсаты сәйкес синтез әдістемесін және оның негізінде АҚ қатерлерді бағалау және талдау жүйелерін құру болып табылады.

Бұрыннан белгілі әдістемені құру тәсілдерін [85] және логикалық–лингвистикалық тәсілін қолдана отырып [85], 2.3 және 2.4 тарауларда берілген әдістер негізінде, сондай–ақ, 2.1 тараудағы қатердің негізгі сипаттамалар үлгілері арқылы ақпараттық қауіпсіздік қатерлерді бағалау және талдау жүйелерінің синтез әдістемесі ұсынылады (3.1 сурет).

Ол келесі он екі кезеңнен тұрады:

1) қатерлерді бағалау және талдау әдісін таңдау;

2–5) ақпараттық қорларды (АР), әрекеттерді, оқиғалар мен қатердің негізгі сипаттамаларын идентификациялау;

6–7) қатер деңгейлерін (ҚД) және негізгі сипаттамалар деңгейлерін қалыптастыру;

8–9) ағымдық мән және мәнділік деңгейін анықтау;

10) ағымдық мәндерді жіктеу;

11–12) ҚД бағалау және талқылау.

Айтылып өткен кезеңдерге жеке–жеке тоқталып өтелік.

1–кезең. Ақпараттық қауіпсіздік қатерлерін бағалау және талдау әдісін таңдау. Бірінші кезеңде ҚД бағалау үшін сарапшыға бағалауды жүзеге асыратын ортаға тәуелді, соның ішінде оның бағаланылатын параметрлер мәндерімен салыстырмалы түрде нақты (бинарлы) артықшылықтары бар жағдайларға байланысты таңдау әдісін іске асыру керек.

Осыларға байланысты әдістеме АҚ қауіптерін бағалау және талдауды FirstM 2.3. тарауда қолданылатын детерминдендірілген ортада және SecondM 2.4. тарау негізіндегі анық емес ортада жүргізуге мүмкіндік береді. Жүзеге асырылған таңдауға тәуелді (бұдан әрі әдістеме деп аталады) мәндердің

аралықтары қалыптастырылады, ағымдық мәндердің жіктелуі жасалынады және алынған нәтижелердің түсіндірілуі жүзеге асады.

2–кезең. Ақпараттық қорларды идентификациялау. Екінші кезеңде қатерлерді бағалау үшін ақпараттық қауіпсіздік идентификациясы орындалады. Ол үшін осындай қорлардың мәліметтер қорларын (МҚ) құру керек. Одан соң одан сарапшылар нысан үшін қатерлерді бағалауға мүмкіндік жасайтын IR_h $h=\overline{1,r}$ (мұндағы h – АР ағымдық идентификатор көрсеткіші (нөмірі), ал r – АР саны) таңдайды. Мысалы, осы кезеңді өту нәтижесінде шығыстың келесі АР болады: IR_1=«Мәліметтер қоры серверi», IR_2=«Принтер», IR_3=«Желілік файл–сервер» және т.б.

3–кезең. Әрекеттерді идентификациялау. Үшінші кезеңде АҚ бұған дейінгі кезеңдерінде идентификацияланған әрбірімен салыстырмалы түрде мүмкін болатын әрекеттерді идентификациялауды жүргізеді $\boldsymbol{BC_1}=\bigcup_{i=1}^{bc_1} BC_{1i}\ (bc_1=\overline{1,n})$, мұндағы, bc_1 – қатердің ағымдық идентификаторының көрсеткіші (нөмірі) 2.1 тарауды қарау, n – қатерлер саны.

Ол үшін екінші кезеңмен сәйкес сарапшылар BC_{1bc_1} таңдауын жүзеге асыратын әрекеттердің МҚ құру керек. Мысалы, IR_1=«Мәліметтер қоры серверi» үшін n=3 болған жағдайдағы кезеңнің шығысында келесі мәліметтер идентификцияланды $\boldsymbol{BC_1}=\bigcup_{i=1}^{bc_1} BC_{1i}\ (bc_1=\overline{1,3})$. Мұндағы, BC_{11}=«Аппараттық ақпараттық қауіпсіздіклар мен сәтсіздіктер»; BC_{12}=«Қаскүнемдік»; BC_{13}=«Қайта жүктеулер» және т.б.

4–кезең. Оқиғаларды идентификациялау. Төртінші кезеңде АҚ бұзылуларының $\mathrm{BC}_2=\bigcup_{i=1}^{bc_2} BC_{2i}\ (bc_2=\overline{1,7})$ оқиғасын идентификциялау қажет. Мұндағы, bc_2 – ағымдағы оқиға идентификаторының көрсеткіші (нөмірі). Соның ішінде алдыңғы кезеңдерде идентификацияланған АҚ–дан әрбір BC_{1bc_1} әсер ететін қауіпсіздік сипаттамаларын идентификциялау керек. [85] қауіпсіздіктің үш сипаттамасы анықталды. Олар – құпиялылық, тұтастық және қол жетімділік. Соған сәйкес 2.1 тарауда берілген bc_2=7 болған жағдайдағы оқиғалардың негізгі идентификаторлары сипатталды. Осы кезеңнің нәтижесінде IR_h, BC_{1bc_1}, BC_{2bc_2} жиынтықтарын аламыз. Мысалы, IR_1 үшін BC_{11}, BC_{12}, BC_{13} анықталады. Сәйкесінше, BC_{27}= «ҚТҚЖБ», BC_{25}= «ТҚЖБ», BC_{23}= «ҚЖБ» болады.

5–кезең. Негізгі сипаттамаларды идентификациялау. Бұл кезеңде бағалау кезіндегі сарапшының мүмкіндіктерін құру үшін кең ауқымды

шамаларды қолдануда 2.1. тараудағы ҚКМ үлгісін қолдану ұсынылады. Соған байланысты негізгі сипаттамалар жиынтығын толық қолдану керек. Олар қатерлерді бағалау кезінде пайдаланылады.

$$\boldsymbol{EC}_{Fh} \in \{EC_i\} = \{BC_3, BC_4, BC_5, BC_6\}$$

Мұндағы, $i = \overline{1,g}$, i – ағымдағы негізгі сипаттама идентификаторының көрсеткіші (нөмірі), ал g – осы сипаттамалардың саны. Бұл кезеңнен өту нәтижесі негізгі сипаттамалар жиынтығының қалыптастырылған жиыны болып табылады. Олар 8–10 кезеңдерде қатерлерді бағалау және талдауда қолданылады.

6–кезең. Қатер деңгейіне (ҚД) арналған өлшемдерді қалыптастыру. Аталмыш кезеңде <*LR*, $\underset{\sim}{T}_{LR}$, X_{LR}> кортеждеріне сәйкес келетін [85] лингвистикалық айнымалының (ЛА) «ҚАТЕР ДЕҢГЕЙІНІҢ» (***LR***) анықталуы қарастырылады. Оның негізгі терм–жиыны $\underset{\sim}{\boldsymbol{T}}_{LR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{LR_j}$ беріледі. Мұндағы, $j = \overline{1,m}$, m – термдер саны. Мысалы, m=3 болған жағдайда, $\bigcup_{j=1}^{3} \underset{\sim}{T}_{LR_j} = \{$«Төмен», «Орташа», «Жоғары»$\}$ болады. Термдерді анықтап болғаннан кейін $X_{DR} \in \{0, max_{LR}\}$ әмбебап жиыны беріледі. Мұнда FirstM әдісін таңдаған жағдайда әрбір $\underset{\sim}{T}_{LR_1}, \ldots, \underset{\sim}{T}_{LR_j}, \ldots, \underset{\sim}{T}_{LR_m}$ термдері үшін $[lr_{min}; lr_1[, \ldots, [lr_m; lr_{max}]$ өзіндік аралық мәндері анықталады. Ал, SecondM әдісі таңдалған болса, онда ***LR*** аралық мәндерімен салыстырмалы түрде эталондық АЕЖ анықталады. Олардың саны қолданылып отырған термдер санына байланысты болады. Егер ***LR*** үшін олар m болса, онда аралықтар саны G=2m–1 болады, жалпы көрінісі $[b_{11}; b_{21}[$, $[b_{21}; b_{12}[$, $[b_{12}; b_{22}[$, …, $[b_{2m-1}; b_{1m}[$, $[b_{1m}; b_{2m}]$ ($j = \overline{1,m}$) түрде болады, ал, мүшелік функциясы (МФ) $\mu_j(lr)$ болады [85]. Осындай әдістермен қалыптастырылған аралықтар, термдер, АЕС және МФ он екінші кезеңде ***LR*** интерпретациялау үшін қолданылады.

7–кезең. $\boldsymbol{EC_i}$ арналған өлшемдерді қалыптастыру. Бұл кезеңде EC_i деңгейін анықтау үшін ЛА–ның «EC_i ДЕҢГЕЙІ» (C_{EC_i}) қалыптасады. Ол < C_{EC_i}, $\underset{\sim}{T}_{C_{EC_i}}$, X_{EC_i} > кортежі арқылы анықталады [83]. Мұндағы, негізгі терм–жиындар $\underset{\sim}{\boldsymbol{T}}_{C_{EC_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{C_{EC_i j}}$ термдердің m арқылы анықталады. Мысалы, m=3 болған жағдайда,

$$\bigcup_{j=1}^{3} \underset{\sim}{T}_{C_{EC_i j}} = \{\text{«Төмен», «Орташа», «Жоғары»}\}$$

болады. Олар лингвистикалық түрде EC_i деңгейін сипаттайды және $X_{EK_i} \in \{0, \max_{C_{EC_i}}\}$ әмбебап жиынында бейнеленеді.

Егер $\underset{\sim}{T}_{C_{EC_i1}}$,…, $\underset{\sim}{T}_{C_{EC_im}}$ үшін FirstM әдісін (1 кезеңді қараңыз) таңдаған жағдайда әрбір EC_i үшін $[c_{EC_i\min}; c_{EC_i1}[$, …, $[c_{EC_ij}; c_{EC_ij+1}[$,…, $[c_{EC_im}; c_{EC_i\max}]$ өзіндік аралық мәндері анықталады. Ал, егер SecondM әдісі таңдалған болса, онда берілген мәндердің толық жиыны анық емес ішкі жиындарға бөлінеді.

C_{EC_i} үшін АЕС–ны аралық мәндермен салыстыра отырып, $[b_{11}; b_{21}[$, $[b_{21}; b_{12}[$, $[b_{12}; b_{22}[$, …, $[b_{2m-1}; b_{1m}[$, $[b_{1m}; b_{2m}]$ ($j=\overline{1,m}$) аралық мәндерімен және $\mu_j(c_{EC_i})$ мүшелік функциямен (МФ) салыстырмалы түрде бейнелеуге болады.

EC_i деңгейіне арналған айтылған тәсілдермен қалыптастырылған аралықтар, термдер, АЕС және МФ оныншы кезеңде пайдаланылады.

8–кезең. Мәнділік деңгейін анықтау. Сегізінші кезеңде негізгі сипаттамалардың мәнділік деңгейлері анықталады. Бұл кезеңде бесінші кезеңде қалыптастырылған $\{EC_i\}$ негізінде әрбір сипаттаманы оның маңыздылық деңгейіне LS_i ($i=\overline{1,g}$) сәйкес қойылады. Егер барлық LS үшін 2.3 тараудағы (1) реттегі қатынас ақиқат болса, онда Фишберн ережесі бойынша i–ші сипаттама мәні 2.3. тараудағы (2.2) бойынша анықталады. Егер барлық негізгі сипаттамалар тең мәнді болса, яғни, $LS_i = LS_{i+1}$ немесе жүйенің артықшылығы болмаса, онда $LS_i = 1/g$ орындалады. Бұл кезеңде LS_i алынған нәтижелер он бірінші кезеңде қолданылады.

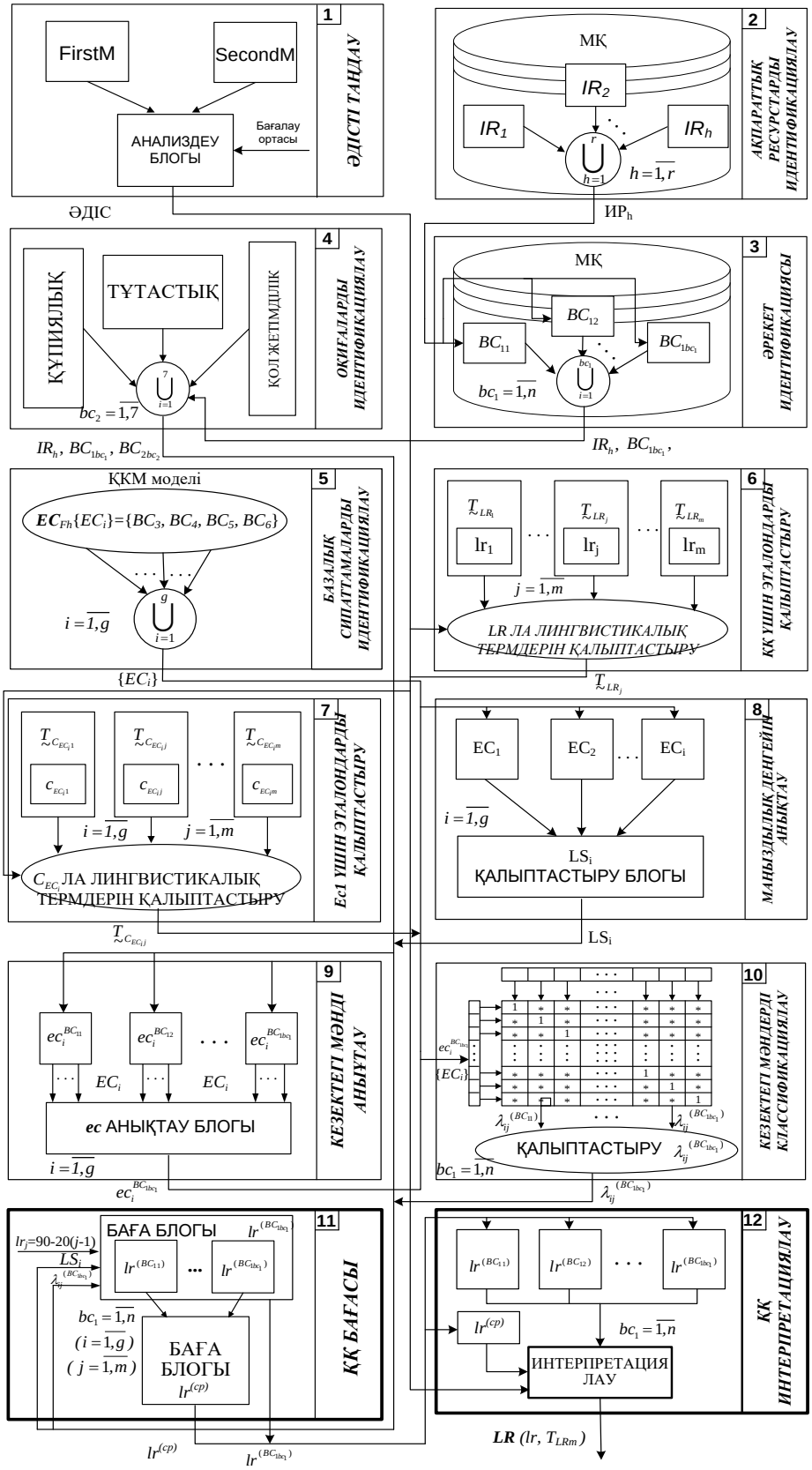
9–кезең. Ағымдық мәнін анықтау. Тоғызыншы кезеңде бесінші кезеңде анықталған жетінші кезеңде қалыптастырылған C_{EC_i} аралықтар мен термдерді қолданатын әрбір $\{EC_i\}$ ($i=\overline{1,g}$) негізгі сипаттамалар бойынша арнайы сарапшылар үшінші кезеңде табылатын барлық BC_{1bc_1} ($bc_1=\overline{1,n}$) үшін ***ec*** анықтайды, яғни:

$$\{ec_i^{BC_{1bc_1}}\}=\{ec_{BC_3}^{BC_{1bc_1}}, ec_{BC_4}^{BC_{1bc_1}}, ec_{BC_5}^{BC_{1bc_1}}, ec_{BC_6}^{BC_{1bc_1}}\}.$$

Мәндер сарапшылардың таңдаулары арқылы, статикалық мәліметтер көмегімен және т.б. арқылы қойылады.

10–кезең. Ағымдық мәндерді жіктеу. Бұл кезеңде жетінші кезеңде қалыптастырылған берілген аралыққа тиістілігі $ec_i^{BC_{1bc_1}}$ анықталады. Одан әрі FirstM және SecondM сәйкес 2.3 тараудағы (2.4) және 2.4 тарауда берілген (2.9) формулалардағы λ мәні қалыптастырылады. Осы тәсілмен барлық BC_{1bc_1}. түрлендіріледі. Осы кезеңде алынған шығым мәліметтер ҚД бағалауда қолданылады.

11–кезең. ҚД бағалау. Бұл кезеңде ҚД–ді бағалау жүзеге асырылады. Бұл жағдайда сәйкесінше 4, 8, 10 кезеңдерде қалыптастырылатын IR_h, BC_{1bc_1}, BC_{2bc_2}, LS_i және $\lambda_{ij}^{(BC_{1bc_1})}$ жиынтықтарын қолдану керек.



Сурет 3.1 – ҚБАҚ Ақпараттық қауіпсіздік синтез әдістемесінің сызбасы

Одан әрі қарай 2.3 тараудағы (2.5) формула бойынша lr_j=90–20(j–1) есептей отырып, әрбір BC_{1bc_1} үшін $lr^{(BC_{1bc_1})}$ ақпараттық қауіпсіздік бұзылуының ҚД көрсеткіші мен 2.3 тараудағы (2.7) формула бойынша оның ақпараттық қауіпсіздік бойынша $lr^{(cp)}$ орташа мәні анықталады.

12–кезең. ҚД талқылау. Он екінші соңғы кезеңде алтыншы кезеңде FirstM және SecondM сәйкес 2.3 тараудағы (2.6) және 2.4 тарауда берілген (2.10) формулалар арқылы алынған, өзгеріске ұшыраған ҚД анықтаудағы эталондық мәндерге байланысты $lr^{(BC_{1bc_1})}$ және $lr^{(cp)}$ табылады. Оның шығыс мәліметтері лингвистикалық және сандық түрде беріледі.

Одан әрі 2 – 4, 9 – 12 кезеңдердің нәтижелері бейнеленетін есеп дайындалады. Қалыптастырылған құжат түріндегі алынған мәліметтер ақпаратты қорғау жүйелерін жасауда ақпараттық жүйелердің түрлі класстары үшін қатерлер үлгісін құруда қолданыла алады. Ол осы үрдісті автоматтандыруға мүмкіндік береді.

3.2. First – ҚБАҚ жүйесі

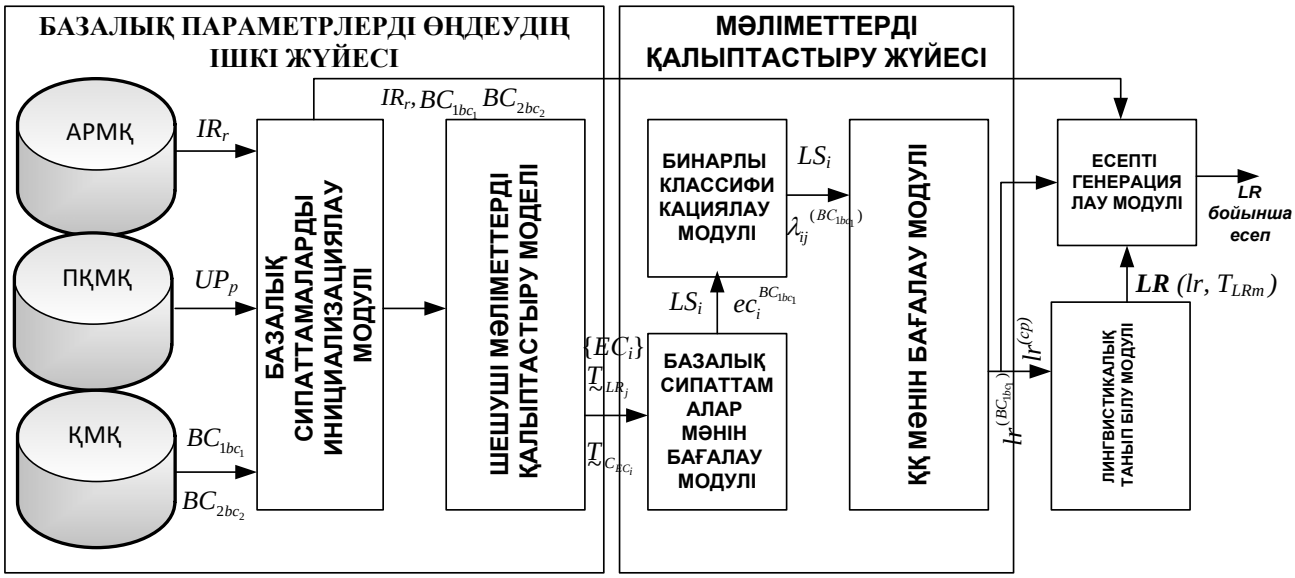
Ұсынылып отырған әдістеменің көмегімен First – ҚБАҚ және Second – ҚБАҚ жүйелері жасалынды. Олардың көмегімен тек бағаланатын параметрлерді нақты анықтайтын сарапшы мүмкіндіктерін ғана емес, сонымен қатар олардың пайымдаулар сенімсіздігін де ескеретін түрлі шығыс шамалар негізінде бағалауды жүргізуге болады.

First – ҚБАҚ жүйесінің құрылымдық сызбасы келесі бөліктерді қамтиды (3.2 сурет): негізгі параметрлерді өңдеу ішкі жүйелері (НПӨІЖ) және мәліметтерді қалыптастыру ішкі жүйелері (МҚІЖ), лингвистикалық тану модулдері (ЛТМ), есептерді араластыру (ЕГМ). Олар негізгі сипаттамалар мәндерімен салыстырғандағы сарапшылардың нақты (бинарлы) пайымдаулары болу шартында қатерлерді бағалау және талдау үшін қолданылады.

Құрылған әдістемеге сәйкес (2–4 кезеңдер) мәліметтерді дайындауда қолданылатын МҚІЖ үшін сарапшылар пайымдауларынна негізделген НПӨІЖ құрылады. Ол АҚ мәліметтер қорынан (МҚ) (АҚМҚ), МҚ қатерлерінен (МҚҚ) және жоба қолданушыларының МҚ (ЖҚМҚ), негізгі сипаттамалардың инициализациялау модулінен (НСИМ), кілттік мәліметтерді қалыптастыру модулінен (КМҚМ) тұрады.

АҚМҚ мәліметтер қоры сәйкесінше $IR \in \{IR_h\}\,(h = \overline{1,r})$ жиынының тізімінен тұрады. Мұндағы, h – АҚ ағымдағы идентификатор көрсеткіші (нөмірі), ал r – АҚ саны. МҚҚ $\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i}\,(bc_1 = \overline{1,n})$ және $\mathrm{BC}_2 = \bigcup_{i=1}^{bc_2} BC_{2i}\,(bc_2 = \overline{1,7})$ жиындарынан тұрады. Бұл жердегі bc_1 – 2.2 тарауда қарастырылған ағымдағы қатер идентификаторының көрсеткіші (нөмірі), n – қатерлер саны, bc_2 – ағымдағы оқиға идентификаторының көрсеткіші (нөмірі).

ЖҚМҚ $UP \in \{UP_p\}\,(p=\overline{1,c})$ жиынының тізімінен тұрады. Мұндағы, p – ағымдағы тұтынушылар жобасы (ТЖ) идентификаторының көрсеткіші (нөмірі), c – олардың саны. Ол 3.3–суретте берілген құрылымдық түрдегі кезекті бағалаудың ТЖ қолдануға мүмкіндік беретін жеке кестелердегі алдыңғы бағалауға байланысты алынған нәтижелерді сақтауға арналған. АҚМҚ қалыптастыруда Commercial көрінісі үшін CRAMM әдісін сипаттау кезіндегі қорлар жіктелуін пайдалануға болады, ал, МҚҚ қалыптастыруда [60, 61] жіктелуін қолдануға болады. НСИМ модулі АҚМҚ және МҚҚ–нен сәйкесінше IR және BC_{1bc_1}, BC_{2bc_2} бағалау нысаны үшін таңдауды жүзеге асыруға арналған. КМҚМ модулі әдістеменің 5–7 кезеңдеріне байланысты жүзеге асады. Ол лингвистикалық айнымалыларды (ЛА) қалыптастыру үшін қолданылады: ЛА $<LR,\ \underset{\sim}{T}_{LR},\ X_{LR}>$, $<C_{EC_i},\ \underset{\sim}{T}_{C_{EC_i}},\ X_{EC_i}>$ кортеждеріне сәйкес анықталатын [60, 61] «ҚАТЕР» (***LR***) және «EC_i ДЕҢГЕЙІ» (C_{EC_i}). Мұндағы негізгі терм–жиын m термдермен $\underset{\sim}{\boldsymbol{T}}_{LR}=\bigcup_{j=1}^{m}\underset{\sim}{T}_{LR_j}$ және $\underset{\sim}{\boldsymbol{T}}_{C_{EC_i}}=\bigcup_{j=1}^{m}\underset{\sim}{T}_{C_{EC_i}j}$ $(j=\overline{1,m})$ беріледі. Бұл жерде сонымен қатар $\boldsymbol{EC}_{Fh}\in\{EC_i\}=\{BC_3,\ BC_4,\ BC_5,\ BC_6\}$ толық жиынынан негізгі сипаттамалар санын таңдау жүргізіледі. Мұндағы, $i=\overline{1,g}$, i – бағаланатын құраушы идентификаторы, g – осы құрауыштар саны, Fh – он алтылық санау жүйесінде берілген код, бинарлы мән [60, 61] жиындағы негізгі сипаттамалардың реттік нөмірін бейнелейді. Түрлендірулер нәтижесінде модуль шығыс нүктесіне $\{EC_i\}$ ЛА ***LR***, C_{EC_i} және олардың терм–жиыны, сонымен қатар, келесі жіктеулерге арналған сәйкесінше аралықтары және лингвистикалық түсіну келіп түседі.



Сурет 3.2 – First– ҚБАҚ жүйесінің құрылымдық сызбасы

Одан соң МҚІЖ–де ҚД қатер деңгейін одан әрі бағалауға арналған мәліметтер қалыптасады. Ол әдістеменің 9 және 8 кезеңдеріне сәйкес негізгі сипаттамалар мәндерін бағалау модулінен (НСМ) және олардың $LS_i \ \ i=\overline{1,g}$ мәндер деңгейлерін анықтаудан, әдістеменің онынші кезеңіне байланысты алынған НСМ $ec_i^{BC_{1bc_1}}$ нәтижесі көмегімен 2.3 тараудағы (2.4) өрнек бойынша $\lambda_{ij}^{(BC_{1bc_1})}$ мәнін қалыптастыратын бинарлы жіктеу модулінен (БЖМ), 2.3 тараудағы (2.5) формула бойынша әрбір идентификацияланған бағалауды $lr^{(BC_{1bc_1})}$ BC_{1bc_1} $(bc_1=\overline{1,n})$ жүзеге асыратын ҚД мәнін бағалау модулінен (МҚД) және 2.3 тараудағы (2.7) формуламен анықталатын оның ақпараттық қауіпсіздік бойынша оның $lr^{(cp)}$ орташа мәнінен тұрады. Ол сарапшылардың ағымдағы мәндерді $ec_i^{BC_{1bc_1}}$, яғни, $\{ec_i^{BC_{1bc_1}}\}=\{ec_{BC_3}^{BC_{1bc_1}}, ec_{BC_4}^{BC_{1bc_1}}, ec_{BC_5}^{BC_{1bc_1}}, ec_{BC_6}^{BC_{1bc_1}}\}$ анықтау үшін қолданылады. Мұндағы, $\boldsymbol{BC_1}=\bigcup_{i=1}^{bc_1} BC_{1i}$ $(bc_1=\overline{1,5})$.

Name	Type	Length	Decimals	Allow Null
id	int	11	0	☐
resource	varchar	200	0	☐
threat	varchar	200	0	☐
probability	int	5	0	☐
frequency	decimal	4	2	☐
loss	decimal	4	2	☐
danger	int	5	0	☐
dr	decimal	4	2	☑

Сурет 3.3 – Тұтынушылар жобасы кестесінің мысалы

ЛТМ модулі оның терм–жиыны және 2.3 тараудағы (2.6) аралық өрнегінің негізінде қалыптастырылған ЛА ***LR*** көмегімен $lr^{(BC_{1bc_1})}$ және $lr^{(cp)}$ мәндерін лингвистикалық түсіндіру үшін қолданылады.

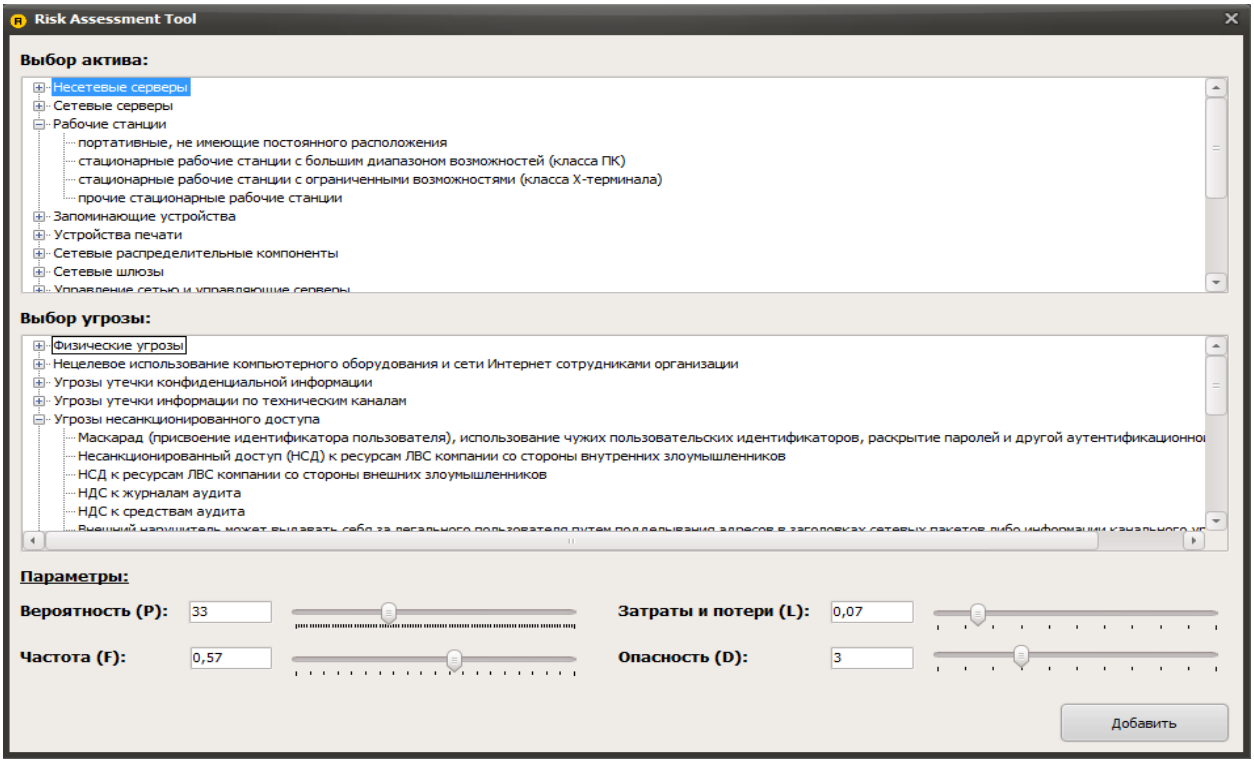
ЕГМ модулі екі ішкі жүйелердің жұмысының нәтижесінде барлық идентификацияланған IR_h, BC_{1bc_1}, BC_{2bc_2} және $lr^{(BC_{1bc_1})}$, $lr^{(cp)}$ бағалау нәтижелері мен олардың лингвистикалық эквиваленті енетін ҚД бағалау есебін аралас етуге мүмкіндік береді.

Жүйенің қызмет етуіне тоқталып өтелік. НСИМ–ға АҚМҚ және МҚҚ–лардан сарапшы таңдайтын бастапқы мәліметтер (БМ) келіп түседі. ЖҚМҚ–дан дайын ТЖ қолдану мүмкіндігі бар. Бұл жерде МҚБЖ MySQL басқарылатын үш МҚ қолданылады: біріншісі АҚ (resources) қамтитын МҚ, екіншісі (threat) қатерлер (әрекеттер) тізімін қамтиды, ал, үшіншісі ТЖ. Алғашқы екі МҚ–ларының құрылымдары бірдей болады. Олардың құрылымдары 3.4–суретте береліп отыр.

Name	Type	Length	Decimals	Allow Null	
id	int	10	0	☐	1
name	varchar	200	0	☐	
id_par	int	10	0	☐	

Сурет 3.4 – АҚМҚ және МҚҚ кестелерінің құрылымдары

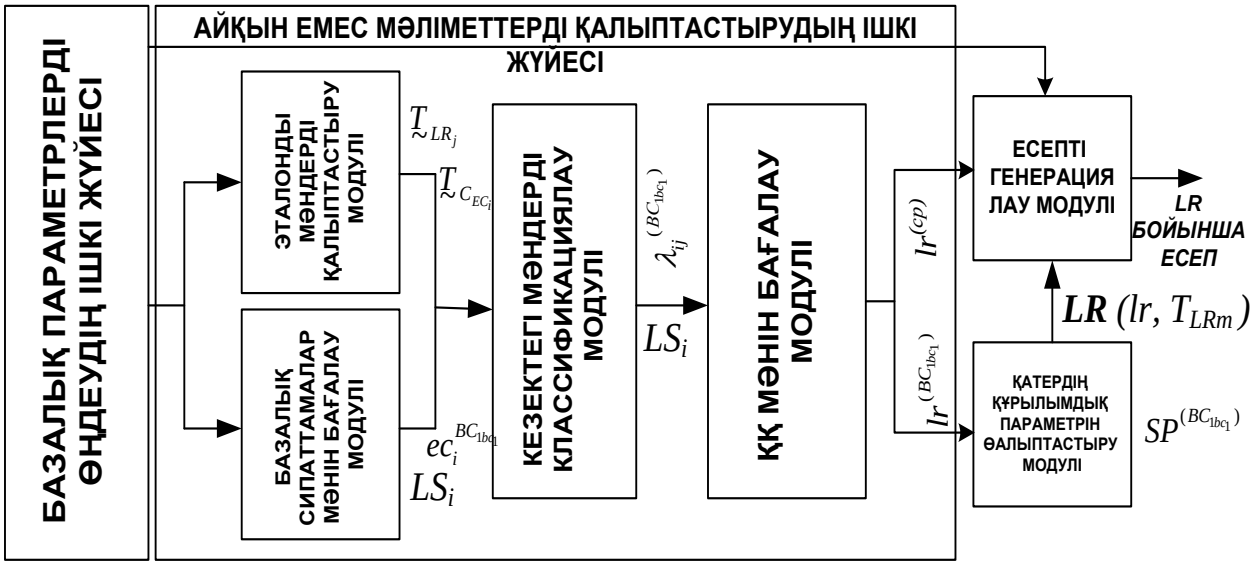
Одан әрі КМҚМ–де LR және C_{EC_i} ЛА кілттік мәндер, $\underset{\sim}{T}_{LR_j}$ және $\underset{\sim}{T}_{C_{EC_i}}$ термдерде бағалау үшін сәйкесінше аралықтар, сондай–ақ, $\{EC_i\}$ саны қалыптасады. ЛА C_{EC_i} және $\{EC_i\}$ мәліметтері МБХ–ға беріледі. Ол жерде $ec_i^{BC_{1bc_1}}$ анықталады (2.5. сурет). Ол үшін модульге қосымша НСИМ–ден нәтижелік шамалар, атап айтатын болсақ, BC_{1bc_1} идентификацияланған шамалар келіп түседі. НСМ–дан шығыс мәндер 2.3 тараудағы әрбір BC_{1bc_1} $(bc_1 = \overline{1,n})$ бинарлы жіктелу үшін БЖМ–ға барады. БЖМ–нан алынған нәтижелер МҚД–ға береледі, нәтижесінде $lr^{(BC_{1bc_1})}$ және $lr^{(cp)}$ есептелінеді. КМҚМ–да қалыптастырылған ЛА мәні МЛР–ге келіп түседі. Онда алынған $lr^{(BC_{1bc_1})}$ және $lr^{(cp)}$ үшін лингвистикалық тану жүзеге асады. Одан кейін ЛТМ, МҚД және НСИМ алынған мәндері көмегімен ЕГМ–да есептер жасалады.



Сурет 2.5 - НСМ–пен жұмыс жасау мысалы

3.3 Second – ҚБАҚ жүйесі

Одан соң Second–ҚБАҚ жүйесі ұсынылады. First–ҚБАҚ жүйесінен айырмашылығы оның көмегімен сарапшы әр уақытта негізгі сипаттамалар қатынасының артықшылықтарын анықтау мүмкін емес болған жағдайда ҚД бағалауға болады. Мұндай жүйенің құрылымдық сызбасы (3.6. сурет) НПӨІЖ, анық емес мәліметтерді қалыптастыру ішкі жүйесінен (АЕМҚІЖ), ЕГМ және қатердің құрылымдық параметрін қалыптастыру модулінен (ҚҚПҚМ) тұрады.



Сурет 3.6 – Second–ҚБАҚ жүйесінің құрылымдық сызбасы

НПӨІЖ функциялары First–ҚБАҚ жүйесіндегі ішкі жүйелерге ұқсас келеді, ал, АЕМҚІЖ ҚД бағалау үрдісінде сарапшының сенімсіздік жағдайын кіріс шамаларда ескеруге мүмкіндік жасайтын анық емес мәліметтерді түзеді. АЕМҚІЖ ішкі жүйелері эталодық мәндерді қалыптастырушы модульдерді (ЭМҚМ), НСМ–ды, ағымдық мәндердің жіктелуі модулін (АМЖМ) және МҚД–ні қамтиды. ЭМҚМ модулі әдістеменің алтыншы және жетінші кезеңдеріне сәйкес ЛА термдері туралы сарапшылардың қабылдаған шешімдеріне байланысты АЕС эталонды МФ құру үшін қолданылады. Мұнда сарапшылар 2.4 тараудағы (2.8) өрнек арқылы және өзінің артықшылығы негізінде мәндер аралығына байланысты ЛА ***LR*** және C_{EC_i} үшін эталондық АЕС анықтай алады. Олардың саны қолданылып отырған термдер санына байланысты болады. Егер олардың саны *m* болса, онда ***LR*** үшін аралықтар саны $G=2m-1$, жалпы $[b_{11};\ b_{21}[, [b_{21};\ b_{12}[, [b_{12};\ b_{22}[, \ldots, [b_{2m-1};\ b_{1m}[, [b_{1m};\ b_{2m}]$ ($j=\overline{1,m}$) және ҚФ $\mu_j(lr)$, түрінде болады. Ал, C_{EC_i} үшін аралықтар саны былай болады: $[b_{11};\ b_{21}[, [b_{21};\ b_{12}[, [b_{12};\ b_{22}[, \ldots, [b_{2m-1};\ b_{1m}[, [b_{1m};\ b_{2m}]$ ($j=\overline{1,m}$) және ҚФ $\mu_j(c_{EC_i})$. Модульдің жұмыс жасауы нәтижесінде ЛА ***LR***, C_{EC_i} және олардың аралықтары, сонымен қатар, АЕС және ҚФ анықталады. НСМ модулінің қызметі First–ҚБАҚ жүйесінің модульдеріне ұқсайды. АМЖМ ЭМҚМ

көмегімен берілген АЕС бойынша $ec_i^{BC_{1bc_1}}$ нысанның анықталушылығы жүзеге асырылатын сарапшылар арқылы анықталған ЛА C_{EC_i} эталондық мәндер негізінде параметрлердің анық емес және анықталған мәндерді алуға мүмкіндік жасайды. Ол арқылы 2.4 тараудағы (2.9) өрнегін қолдана отырып, λ мәнін есептеп табуға болады. Осындай жолмен First–ҚБАҚ жүйесінде LS_i анықталады. Модульдің жұмысы нәтижесінде НСИМ және LS_i–дегі әрбір идентификацияланған BC_{1bc_1} арналған $\lambda_{ij}^{(BC_{1bc_1})}$ мәнін аламыз. Мұндағы МҚД модулінде First–ҚБАҚ жүйесіндегі МҚД модуліне қарағанда изоморфты функциялар болады. Одан мәліметтер ҚҚПҚМ–ға келіп түседі. Мұнда $lr^{(BC_{1bc_1})}$, $lr^{(cp)}$ мәндерін есептеу және 2.4 тараудағы (2.10) өрнегінің көмегімен тұрғызылған эталондар арқылы $SP^{(BC_{1bc_1})}$ құрылымдық параметрлер анықталады. Оның көмегімен ҚД сандық мәнін және ағымдағы негізгі құрауыштар мәнін жасайтын сарапшының сенімсіздігін есепке алатын $\lambda_{ij}^{(BC_{1bc_1})}$ параметрі арқылы одан әрі жіктеуге болатын лингвистикалық интерпретацияны алуға болады. ЕГМ модулі де First–ҚБАҚ жүйесінің модуліне ұқсас келеді. Ол қорытынды есептерді араластырып отырады.

Енді Second–ҚБАҚ жүйесінің жұмыс жасауын сипаттап өтетін болсақ. НПӨІЖ функциясы First–ҚБАҚ жүйесіндегі ішкі жүйелерге ұқсас болады. КМҚМ–нан алынған $\underset{\sim}{T}_{LR_j}$, $\underset{\sim}{T}_{C_{EC_i}}$, $\{EC_i\}$ мәліметтер ЭМҚМ мен МБХ–ға келіп түседі. ЭМҚМ – да қалыптастырылған ЛА мәндері C_{EC_i}, АЕС эталондар, ҚФ $\mu_j(c_{EC_i})$ және ЛА мәндер аралығы МБХ–да әрбір анықталған $\{EC_i\}$ үшін алдағы бағалауда $ec_i^{BC_{1bc_1}}$ қолданылады. Алынған БМ АМЖМ–ға беріледі. Мұнда КМҚМ және ЭМҚМ–дерден бастапқы нәтижелік мәндер көмегімен $ec_i^{BC_{1bc_1}}$ мәнінің жіктелуі орындалады. Сонымен қатар, АМЖМ–де ағымдық мәндері бар анық емес эталонды салыстыру жүзеге асырылады және 2.4 тарауда берілген (2.9) өрнекке сәйкес $\lambda_{ij}^{(BC_{1bc_1})}$ анықталады. АМЖМ–нан алынған $\lambda_{ij}^{(BC_{1bc_1})}$ МҚД–ға барады. Бұл жерде әрбір BC_{1bc_1} үшін $lr^{(BC_{1bc_1})}$ және $lr^{(cp)}$ анықталады.

Одан әрі БМ ҚҚПҚМ–ға беріледі, онда $SP^{(BC_{1bc_1})}$ анықталады, ал, ЕГМ–да МҚД, ҚҚПҚМ және НСИМ алынған мәліметтер бойынша нәтижелік есеп жасалады.

Барлық қажетті мәліметтер мен нәтижелер қажетті МҚ–на енгізіледі және сенімділігін жоғарылату үшін резерві алынады. Ол оның бағдарламалық коды мен жүйе құрылымын өзгертпей–ақ БМ тез әрі қауіпсіз өзгертуге мүмкіндік береді.

Үшінші бөлім бойынша тұжырым

1. Ұсынылып отырған әдістеменің көмегімен АҚ қатерлерді тиімді бағалау және талдауға арналған бағдарламалық және бағдарламалы–аппараттық жүйелерді құруға болады. Оларды негізгі сипаттамалардың түрлі жиынтықтарының кіріс мәліметтер ретінде қолдануға болады. Олар икемділікті жоғарылатады әрі анықталған және анық емес нашар қалыптастырылған орталарда жобаланып отырған ҚБАҚ мүмкіндіктерін кеңейтеді.

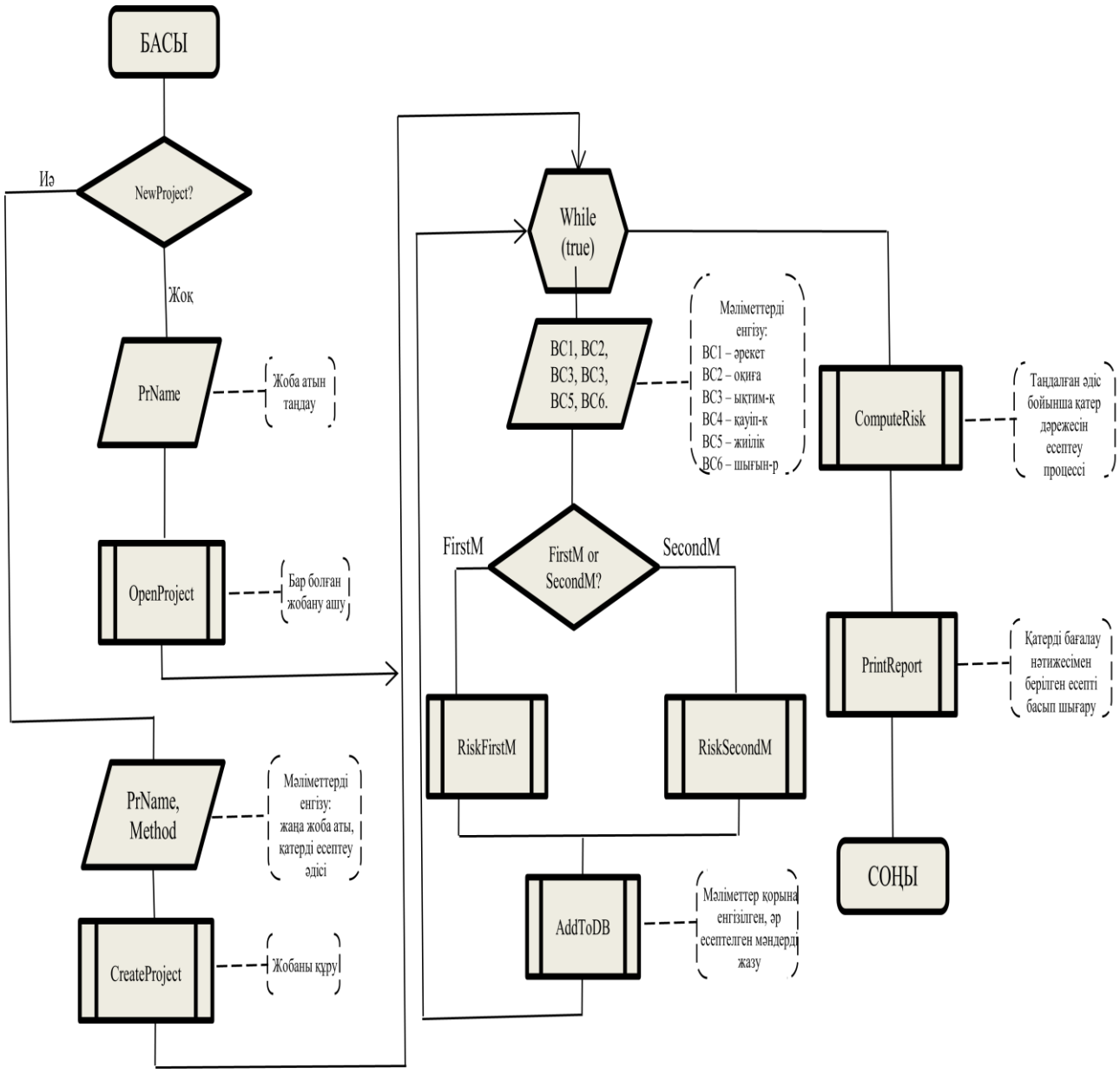
2. Негізгі сипаттамаларды өңдеу ішкі жүйелері негізінде және ұсынылған **FirstM** және **SecondM** әдістері көмегімен жүзеге асырылатын мәліметтерді қалыптастыру арқылы ҚБАҚ АҚ құрылымдық шешімдері жасалды. Олар сандық және сапалық сипаттары негізінде нәтижелік мәліметтерді қалыптастыруға және түрлендіруге мүмкіндік береді.

4 ҚАТЕРДІ БАҒАЛАУ МЕН АНАЛИЗДЕУ ЖҮЙЕЛЕРІН ЭКСПЕРИМЕНТТІК ЗЕРТТЕУ

4.1 Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу жүйесі жұмысының негізгі алгоритмі

Ұсынылып отырған First–ҚБАҚ және Second–ҚБАҚ жүйелерінің құрылымдық сызбалары негізінде автоматтандырылған режімде ақпараттық қауіпсіздік қатерлерін бағалау және талдауға мүмкіндік беретін бағдарлама қосымшасын жүзеге асыруға болады. Олардың жұмыс жасауларының негізгі алгоритмдерін (4.1. сурет) төмендегідей кезеңдерге бөліп қарастыруға болады:

1. жаңа тұтынушылар жобасын (ТЖ) құру немесе бұрыннан бар ТЖ ашу;
2. қолда бар ТЖ атын көрсету;
3. тұтынушылар жобасының мәліметтер қорында сақталынған қолда бар мәліметтер арқылы және сақталған баптау (настройка) арқылы ТЖ ашу;
4. жаңа ТЖ көрсету және FirstM немесе SecondM әдістерін таңдауды жүзеге асыру;
5. таңдалынған параметрлі жобану құру бос (пустой) жобаны жүктеу мен МҚ–ындағы ТЖ кестесін құру арқылы жүзеге асырылады;
6. IR, BC_{1bc_1} таңдау және $ec_i^{BC_{1bc_1}}$ мәнін көрсету;
7. берілген IR_h, BC_{1bc_1} және BC_{2bc_2} жиынтығына арналған $lr^{(BC_{1bc_1})}$ бағалау;
8. МҚ–ғы тұтынушылар мәліметтері мен есептелген $lr^{(BC_{1bc_1})}$ жобасы;
9. ТЖ–ғы әрбір ақпараттық ресурстар үшін $lr^{(cp)}$ есептеу;
10. барлық IR_h және олардың сәйкесінше BC_{1bc_1} көрсету арқылы, сонымен бірге ақпараттық ресурстар үшін $lr^{(cp)}$ туралы ақпараттарды сандық және лингвичтикалық түрде көрсету арқылы, әрбір қауіп жекелей $lr^{(BC_{1bc_1})}$ көрсету арқылы есептерді генерациялау.



Сурет 4.1 – Ақпараттық қауіпсіздік қатерлерін бағалау және анализдеу жүйесінің негізгі алгоритмі

Қалыптастырылған ЕГМ есептер мысалдары сәйкесінше 4.2. суреттің а және б нұсқаларында берілген.

Отчет

по расчету степени риска для активов организации
от 22.06.2015
для проекта
Zero_Condition

Сумарно по активам

Список активов	Степень риска
несетевые серверы общего назначения	НР - 16

Детальная информация по активам

несетевые серверы общего назначения

Угрозы	Степень риска
Физический несанкционированный доступ в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	10
Кража или повреждение компьютерного оборудования и носителей информации инсайдерами	10
Кража или повреждение компьютерного оборудования и носителей информации внешними злоумышленниками	15
Постороннее лицо может получить физический доступ к комплексу средств защиты с целью переконфигурирования либо создания возможности обхода средств защиты	20
Кража бумажных документов инсайдерами	25

а) Second – ҚБАҚ жүйесі

Отчет

по расчету степени риска для активов организации
от 22.05.2015
для проекта
fuz

Сумарно по активам

Список активов	Степень риска
сетевые серверы БД	РН (0,3), РС (0,7) - 37
портативные, не имеющие постоянного расположения	РН (0,25), РС (0,75) - 37,5
принтер	РВ (0,7), ПР (0,3) - 73

Детальная информация по активам

сетевые серверы БД

Угрозы	Степень риска
Физический несанкционированный доступ в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	35
Злоупотребление средствами аудита	39

портативные, не имеющие постоянного расположения

Угрозы	Степень риска

б) First – ҚБАҚ жүйесі

Сурет 4.2 – Жинақталған есеп мысалы

Ұсынылып отырған әдістеме негізінде ақпараттық қауіпсіздік қатерлерін тиімді бағалау және талдауға арналған бағдарламалық және бағдарламалық – аппараттық жүйелерді құруға болады. Оларды негізгі сипаттамалардың түрлі жиынтықтарының кіріс мәліметтері ретінде қолдануға болады. Ол икемділікті жоғарылатады және жобаланып отырған нақты бір нашар қалыптастырылған ортада жұмыс жасайтын ҚБАҚ мүмкіндіктерін кеңейтуге мүмкіндік береді. Осы әдістеме негізінде ҚБАҚ-тың құрылымдық шешімдері анықталды.

Құрылған Second – ҚБАҚ және First – ҚБАҚ жүйелерінің құрылымы негізінде бағдарламалық құралдар (сурет 4.3) жасалды. Олар бұрыннан белгілі 2.2 тарауда берілген айырмашылығы негізгі сипаттамалардың түрлі жиынтықтарының кіріс мәліметтерін қолданады. Ол қолдану мүмкіндіктері мен икемділігін жоғарылатады және жобаланып отырған нақты бір нашар қалыптастырылған ортада жұмыс жасайтын жобаланып отырған ақпараттық қауіпсіздік қатерлерді бағалау және талдау құралдарының мүмкіндіктерін кеңейтеді.

Сурет 4.3– Бағдарламалық өнімнің негізгі терезесі

4.2 First – ҚБАҚ жүйесін зерттеу

Қазіргі уақыттағы IT–технологияның қарқынды дамуына байланысты адам өмірінің барлық қызмет салаларында қолданыс тапқан компьютерлік желілердегі ақпараттық қауіпсіздік қорғау, оның құпиялылығын, тұтастығын және қол жетімділігін бұзуға бағытталған қатерлер саны өсуде. Сондықтан осындай ақпараттық қорлардың қауіпсіздігін сақтау түрлі кәсіпорындарда, фирмаларда, жалпы алғанда мемлекетте басты мәселелердің біріне айналып отыр. Қазіргі таңда мұндай туындаған мәселелерді ақпараттық қауіпсіздік басқару жүйелерінің көмегімен шешуге болады. Ондай жүйені құру үшін жиі жоғарғы анықталмаушылықпен сипатталатын ақпараттық қауіпсіздік қатерлерін бағалауды және талдауды жүзеге асыру керек.

Бұл жағдайда автоматтандырылған режімде қатерлерді бағалауды жүзеге асырудың тиімді құралдарын қолдану қажеттігі туындайды. Ондай мәселені

шешу үшін 2.3 және 2.4 тарауларда қарастырылған логикалық – лингвистикалық тәсілге және 2.1 тараудағы қатарлердің негізгі сипаттамаларының кортеждік үлгісіне негізделген 3.1 тарауда берілген ҚБАҚ ақпараттық қауіпсіздік синтез әдістемесін қолдана отырып, 3.2 және 3.3 тарауларда берілген бағалау жүйесінің жаңадан құрылымдық шешімдері ұсынылды. Жасалған әдістердің практикада қолданылауы мен жүйенің құрылымдық жүзеге асыруына сәйкес түрлі алғашқы шамалар үшін бағалауды жүзеге асыруды қамтамасыз ететін ПҚ ҚБАҚ дайындау бойынша өзекті мәселені шешуді және сарапшының мүмкіндіктерін есепке алуды қажет етеді.

Соған байланысты жұмыстың негізгі мақсаты анықталған және анық емес нашар байланысқан ортада таңдалған негізгі сипаттамалар негізінде ақпараттық қауіпсіздік қатерлерін бағалау және талдауды жүргізуге мүмкіндік беретін бағалау құралдарын құру және қолданысқа енгізу болып табылады.

Алға қойылып отырған негізгі мақсатқа жету үшін ұсынылған 3.2 және 3.3 тарауларда берілген First – ҚБАҚ және Second – ҚБАҚ жүйелердің құрылымдық шешімдеріне байланысты түрлі негізгі сипаттамалар жиынының кіріс мәліметтері негізінде ПҚ құруға негізделеді. Оны пайдалану икемділігін, қолдану қолайлығын, мүмкіндіктердің кеңеюін арттырады және анықталған ортада жұмыс жасайтын құралдардың қызметтерін жоғарылатады. Ол уақытқа байланысты әр түрлі кері әсерлерге өте төзімді болады. Сондай–ақ, бұл құралдар анықталмаушылық, кездейсоқтық, тұрақсыздық, әр түрлі кері әсерлер т.б. дәрежелері өте үлкен болатын анық емес нашар байланысқан орталар жұмыстарына да бағытталған. Ал, ол үрдісті қалыптастыру үшін нақты емес жиындар теориясының математикалық аппараты қолданылады.

Зерттеу жұмысында құрылған ПҚ 3.1 тарауда қарастырылған қатерлерді бағалау және талдау синтез әдістемесі негізінде жүзеге асырылды. Оған сәйкес бірінші кезеңде бағалау әдісін таңдауды жүзеге асыру қажет. Одан әрі қарай әдістемеге сәйкес ақпараттық қауіпсіздік идентификациялау және ақпараттық қауіпсіздік бұзылу әрекеттері мен оқиғалары үшін сәйкесінше мәліметтер қорын (МҚ) жасау қажет етіледі:

– ISO/IEC 27002:2005-дан қатерлер тізімінің негізінде жасалған BC_{1bc_1} ($bc_1 = \overline{1,n}$) әрекеттердің;

– Commercial үшін CRAMM әдісіне сәйкес қорлар тізімін қамтитын IR_h ақпараттық қорлардың;

– базалық сипаттамалардың $ec_i^{BC_{1bc_1}}$ (БС).

Ыңғайлы болу үшін және ПҚ–те алынған нәтижелерді одан кейін де қолдану үшін барлық мәліметтер тұтынушылар жобасында (ТЖ) сақталады. Олар МҚ–да жинақталады. Кіріс мәліметтері негізінде келесілер мәндер келіп түседі:

$$IR \in \{IR_h\}\ (h = \overline{1,20});$$

$$BC_1 \in \{BC_{1bc_1}\}\ (bc_1 = \overline{1,60});$$

$$BC_2 \in \{BC_{2bc_2}\}\ (bc_2 = \overline{1,7}),$$

Ал, мәндер $ec_i^{BC_{1bc_1}}$: $\{ec_i^{BC_{1bc_1}}\}=\{ec_{BC_3}^{BC_{1bc_1}}, ec_{BC_4}^{BC_{1bc_1}}, ec_{BC_5}^{BC_{1bc_1}}, ec_{BC_6}^{BC_{1bc_1}}\}$ болады, мұнда $i=\overline{1,4}$. IR_h және BC_{1bc_1} идентификаторлары олардың тізімдер атауларына сәйкес келетін мәтіндік мәндерді қабылдайды.

First – ҚБАҚ жүйесінің жұмысын қарастырайық. Одан әрі 3.1 тарауда қарастырылған әдістемеге сәйкес бейнеленетін *LR* параметрлі ҚД-ы бағалау оның эталонды мәндерін анықтау арқылы жүзеге асады.

Ұсынылып отырған ПҚ-да қатерлер деңгейлерінің сандық мәндері 0 мен 100 аралығында болады.

LR лингвистикалық түрде келесі мәндер көмегімен бейнеленеді:

– «АҚ бұзу қатер деңгейі өте төмен» (ТҚ);
– «АҚ бұзу қатер деңгейі төмен» (ҚТ);
– «АҚ бұзу қатер деңгейі орташа» (ҚО);
– «АҚ бұзу қатер деңгейі жоғары» (ҚЖ);
– «АҚ бұзу қатер деңгейі өте жоғары» (ЖҚ).

Алынған ДҚ $lr^{(BC_{1bc_1})}$ сандық мәнінен лингвистикалық тану сәйкестілігін анықтау үшін төмендегі (4.1) формула пайдаланылады:

$$\underset{\sim}{T}_{LR}=\begin{cases} \text{Ò}^2\ , егер\ lr^{(BC_{1bc_1})}\in[\,lr_{\min};lr_1[\\ ^2\ \text{Ò}, егер\ lr^{(BC_{1bc_1})}\in[\,lr_2;lr_3[\\ ^2\ \hat{I}\ , егер\ lr^{(BC_{1bc_1})}\in[\,lr_4;lr_5[\\ ^2\ Æ, егер\ lr^{(BC_{1bc_1})}\in[\,lr_6;lr_7[\\ \hat{I}\ ^2\ , егер\ lr^{(BC_{1bc_1})}\in[lr_8;lr_{\max}] \end{cases}, \quad (4.1)$$

Мұндағы [lr_{min}; lr_1[, [lr_2; lr_3[, [lr_4; lr_5[, [lr_6; lr_7[, [lr_8; lr_{max}] [0; 20[, [20; 40[, [40; 60[, [60; 80[, [80; 100] мәндеріне сәйкес келеді. ПҚ – НС үшін эталондық мәндерді анықтау келесі түрде жүргізіледі:

– ***BC₃*** (0 мен 100 аралығындағы мәндерді қабылдайды, сынамаларды алу қадамы 1-ге тең);
– ***BC₄*** (0 мен 10 аралығындағы мәндерді қабылдайды, сынамаларды алу қадамы 1-ге тең);
– ***BC₅*** (0 мен 1 аралығындағы мәндерді қабылдайды, сынамаларды алу қадамы 0,01-ге тең);
– ***BC₆*** (0 мен 0,5 аралығындағы мәндерді қабылдайды, сынамаларды алу қадамы 0,01-ге тең).

Мәнділік деңгейін және ПҚ-ғы ағымдық НС мәнін анықтау кезеңдерінде мәліметтерді енгізу үшін 4.4 суреттің жоғарғы бөлігінде берілген интерактивті интерфейс қолданылады. ПҚ-ғы ҚД бағалау және ағымдық мәндерді жіктеу автоматты түрде жүргізіледі. Әрбір қатер әрекеті үшін $lr^{(BC_{1bc_1})}$ мәнін есептеу келесі өрнек арқылы жүргізіледі:

$$lr^{(BC_{1bc_1})} = \sum_{j=1}^{m}\left(lr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(BC_{1bc_1})} \right),$$

Мұндағы:

$$lr_j = 90 - 20(j-1),$$

$$\lambda_{ij}^{(BC_{1bc_1})} = \begin{cases} 1, \text{егер } ec_i^{BC_{1bc_1}} \in [\, c_{EC_i(j-1)}; c_{EC_i j}[\\ 0, \text{егер } ec_i^{BC_{1bc_1}} \notin [\, c_{EC_i(j-1)}; c_{EC_i j}[\end{cases} (bc_1 = \overline{1,n}),\ LS_i = \frac{2(g-i+1)}{(g-1)g}$$

$(i = \overline{1,g})$ немесе $LS_i = 1/g$ $(j = \overline{1,m})$.

Ақпараттық қауіпсіздік үшін $lr^{(cp)}$ $lr^{(cp)} = (\sum_{bc_1=1}^{m} lr^{(BC_{1bc_1})})/m$ өрнегінің көмегімен есептелінеді.

Алынған нәтижелердің сәйкесінше түсіндірмелері болады, ал ПҚ қажетті есептерді араластырады.

Негізгі функцияларды тестілеу үшін және ПҚ ҚБАҚ жұмыс жасау принципін көрсетуде оның тексеруін Microsoft Windows 7 Home Premium x64 операциялық жүйемен басқарылатын компьютер көмегімен орындау керек. Дайындалған қосымша өзінің жұмыс жасауы үшін жүйелік файлдар мен қосымша кітапханаларды қажет етпейді. Себебі, жобаны орындауда келесі операциялар орнатылады: Use dynamic RTL = false; Build with runtime packages = false. Сонымен қатар, қосымша МҚ қызметі үшін MySQL 5.1.60 x64 сервері орнатылады. Жобаланған ПҚ көмегімен «test24» тестілеу жобасы жасалды. Ал, IR_1 үшін тексеруде **«Желілік серверлер»** бөлімінен **«желілік файл-сервер»** таңдалынып алынды. Тестілеу нақты мәліметтер көзінде яғни, детерминделген ортада жүргізілді.

Берілген ақпараттық қауіпсіздік үшін келесі түрдегі BC_{1bc_1} $(bc_1 = \overline{1,3})$ баптауларды орнату керек:

BC_{11}=«Ақпаратты өңдеу құралдарын теріс пайдалану» («Ұйым қызметкерлерінің компьютерлік құрылғылар мен Интернет желісін толық қолданбау» бөлімі бойынша жүргізіледі);

BC_{12}=«Байланыс желісінде түрлі желілік трафиктерді сараптауыштарды қолдану арқылы ақпараттардың жолда жетпей қалуы» («Құпия ақпараттың жайылып кету қауіп-қатерлері» бөлімі бойынша жүргізіледі);

BC_{13}=«Ақпараттарды тасымалдауыштардың бүлінуі» («Ақпараттық автивтерді және IT–қызметтерінің қол жетімділігін бұзу немесе жоғалту қатерлері» бөлімі бойынша жүргізіледі).

Содан соң әрбір қатерге баланысты $lr^{(BC_{1bc_1})}$ мәндерін есептеу жүргізіледі. Олардың нәтижелері 4.1-кестеде беріліп отыр. Кестеден көріп отырғанымыздай, беріліп отырған барлық қатерлерде ақпараттық қауіпсіздік қатерлерінің деңгейлері төмен деңгейде болады.

Кесте 4.1- First – ҚБАҚ ПҚ бағалау нәтижелері

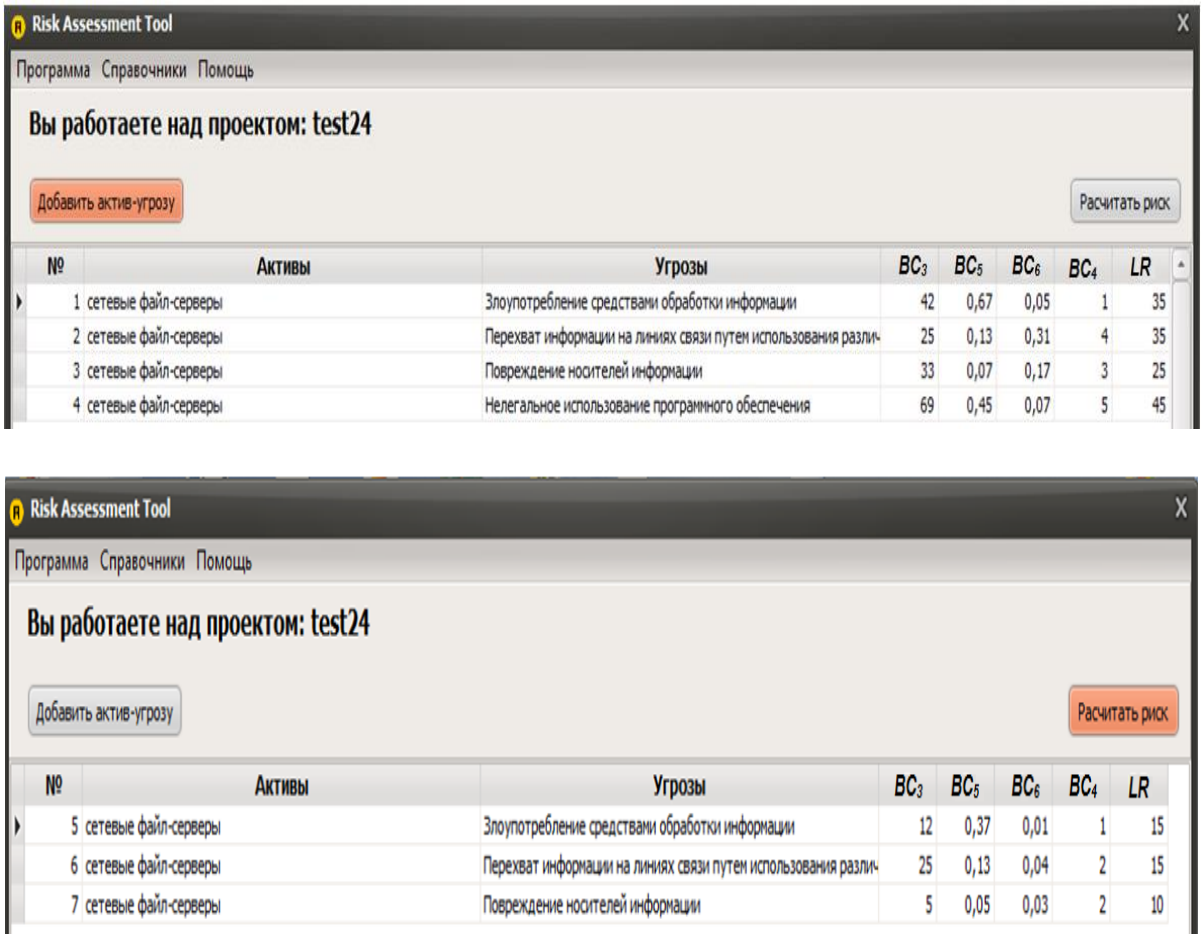
BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	42	1	0,67	0,05	35	*ҚТ*
BC_{12}	25	4	0,13	0,31	35	*ҚТ*
BC_{13}	33	3	0,07	0,17	25	*ҚТ*

Одан әрі беріліп отырған ақпараттық қауіпсіздік үшін $lr^{(cp)}$ орташа мәнін есептеу жүзеге асырылады. Оның нәтижесінде $\underset{\sim}{T}_{LR}$ – ҚТ сәйкес болатын $lr^{(cp)}$ =31,67 аламыз ((4.1) өрнегін қараңыз).

Одан кейінгі ПҚ-ны анықтау бірнеше бағалау орталары күйлерін үлгілеу негізінде жүзеге асады:

1-ші күй – Ақпараттық қауіпсіздік үшін қатерлердің орнатылған санының бастапқы шарттары;

2-ші күй – Ақпараттық қауіпсіздік үшін қатерлер саны көбейтілді;



Сурет 4.4 – First – ҚБАҚ ПС интерактивті интерфейсі

3-ші күй – Ақпараттық қауіпсіздік үшін бір қатерді бұғаттайды;

4-ші күй – негізгі сипаттамалардың мәндерінің өзгерісі (көбеюі немесе азаюы).

1–ші күйде алғашқы шарттар мен ҚД есептеу нәтижелерін қамтиды, олар бірінші кестеде берілген. Келесі күйлерді үлгілеу нәтижелерін қарастырамыз.

2–ші күй ЖҚ–ға IR_1=«Желілік файл-сервер» үшін BC_{14} қосымшасын кірістіру арқылы өзгерістер енгізілді. Яғни, «Заңды қатерлер» бөлімінің BC_{14}=«Бағдарламалық қамтамасыз етуді заңсыз пайдалану» бөлімшесіне енеді. 4.2-кестеде сарапшылардың бағалауы бойынша анықталатын $ec_i^{BC_{1bc_1}}$ мәндері берілген. Нәтижесінде BC_{14} үшін ҚД мәнін есептеулер жүргізіледі, яғни, 4.1. суреттегі бірінші терезеде бейнелетін $lr^{(BC_{14})}$=45, ал BC_{14} интеграциялағаннан кейін орташа $lr^{(cp)}$ мәні $lr^{(cp)}$= 35 тең болды, ол $\underset{\sim}{T}_{LR}$ – ҚТ мәніне сәйкес келді.

Кесте 4.2 - First - ҚБАҚ ПҚ $ec_i^{BC_{1bc_1}}$ мәндері

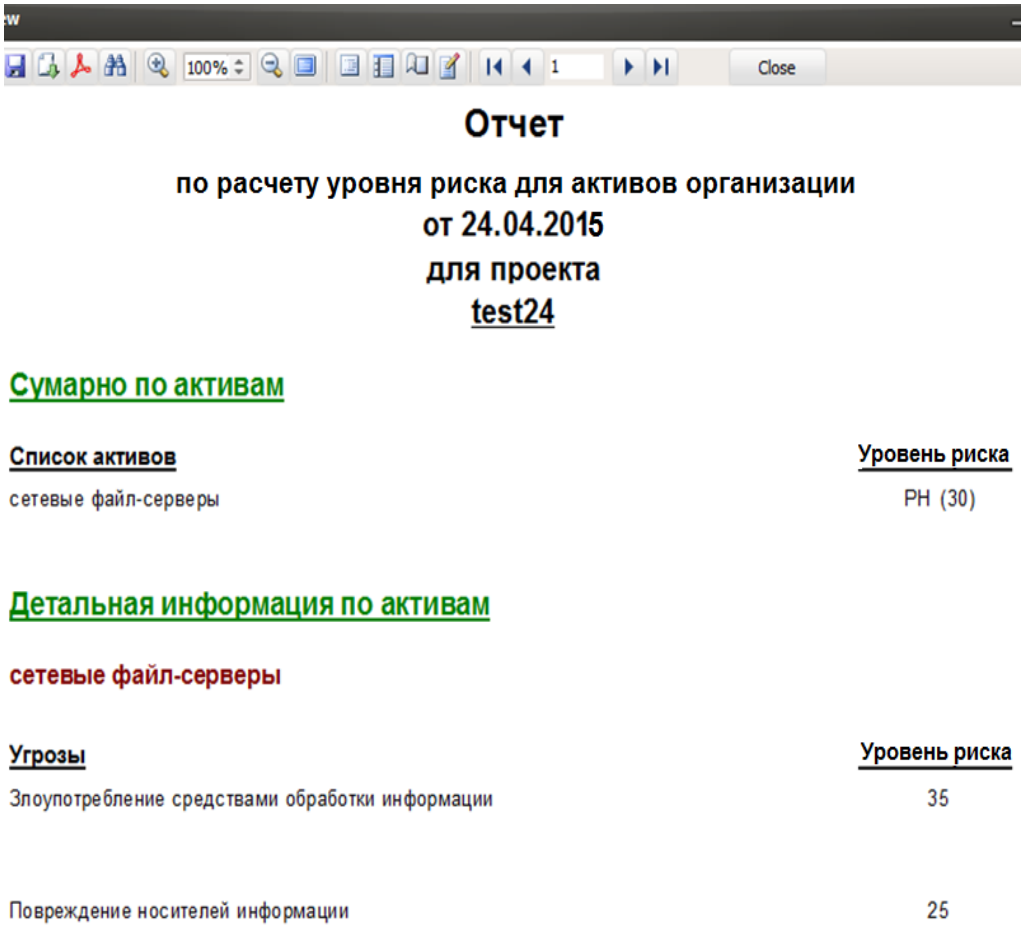
BC_{1bc_1}	BC_3	BC_4	BC_5	BC_5
BC_{11}	42	1	0,67	0,05
BC_{12}	25	4	0,13	0,31
BC_{13}	33	3	0,07	0,17
BC_{14}	69	5	0,45	0,07

3–ші күй. Одан кейін BC_{12}=«Желілік трафикті талдаулардың әр түрлі түрлерін қолдану арқылы байланыс желілерінде ақпараттарды жібермеу» болдырмауға байланысты жасалатын нысанды қорғауды бағалауда үлгілеу жүргізілді. Бұл жерде $lr^{(BC_{1bc_1})}$ және $lr^{(cp)}$ қайталанатын өлшеулер орындалады. Үлгіленетін жағдайларды ескере отырып құрылған жүйені қолданып, IR_1 үшін $lr^{(cp)}$ алынған мәні 30–ға дейін азайды, яғни, $lr^{(cp)}$ $\underset{\sim}{T}_{LR}$ = 30 (ҚТ). Оны 4.5 суретте беріліп отырған, қалыптастырылған, дайындалған құралдар есебінен байқауға болады. Бұл $lr^{(cp)}$ мәні BC_{1bc_1} саны өзгерген кезде өзгереді, ал, ақпараттық қауіпсіздіктің бұзылуы ҚД барлық жағдайлар үшін төмен болып анықталады. Одан әрі жүргізілген тәжірибе нәтижелері BC_{1bc_1} санының айтарлықтай көбейгенінде немесе азайғанында $lr^{(cp)}$ мәні де сәйкесінше өзгеретіндігін көрсетті.

4–ші күй. Есептеулер жүргізілгеннен кейін 1-ші күй бойынша екі жағдай үшін үлгілеу жүргізілді:

– Біріншісінде қорғау нысанында ақпараттық қауіпсіздік қатерлерді бағалау және талдаудың алдыңғы нәтижелері ескеріледі;

– Екіншісінде қорғау нысанында бағалаудың алдыңғы нәтижелері ескерілмейді – қатерлерді азайту үшін оларды енгізуді жүзеге асыратын шешімдер қабылданбайды.



Сурет 4.5 - First – ҚБАҚ ПҚ жинақталған есеп мысалы

Бірінші жағдайды ескере отырып, беріліп отырған АҚ үшін қатерлер деңгейлерін төмендету мақсатында қорғау нысанында көптеген зерттеу әрекеттері жүргізілді. Оларды атап өтетін болсақ:

– BC_{11} = «Ақпараттарды өңдеу құралдарына қиянат жасауды» азайту үшін қолданушыларға олардың қызметтеріне байланысты құқықтары мен мүмкіндіктері берілетін кірісті шектеу жүйесі енгізілді;

– BC_{12}=«Желілік трафикті талдаулардың әр түрлі түрлерін қолдану арқылы байланыс желілерінде ақпараттарды жібермеу» болдырмас үшін желілік трафиктерді шифрлеу жүйесі жасалды;

– Сын ақпараттардың резервті көшірмелерін күнделікті құрып отыратын қатқыл дисктердің жағдайларын бақылауды жүзеге асыратын жүйе жасалды, BC_{13}=«Ақпарат тасуыштардың бүлінуі» бейтараптандыру үшін RAID 1 технологиясы енгізілді.

АҚ қатерлерді бағалау және талдауды қайта жүзеге асырғаннан кейін сарапшылар негізгі сипаттамалардың шамаларын анықтап берді. Ол шамалардың мәндері 4.3-кестеде келтірілді.

Жүргізілген зерттеу өзгерістерінің нәтижелері 4.4. суреттің төменгі терезесінде бейнеленген түрде болады.

Әрбір BC_{1bc_1} үшін қайтадан $lr^{(BC_{1bc_1})}$ мәндерін есептеу жүргізілді. Оның нәтижелері 4.3-кестеде беріліп отыр.

4.3-кесте First – ҚБАҚ ПС бағалау құраушыларының және $lr^{(BC_{1bc_1})}$ мәндері

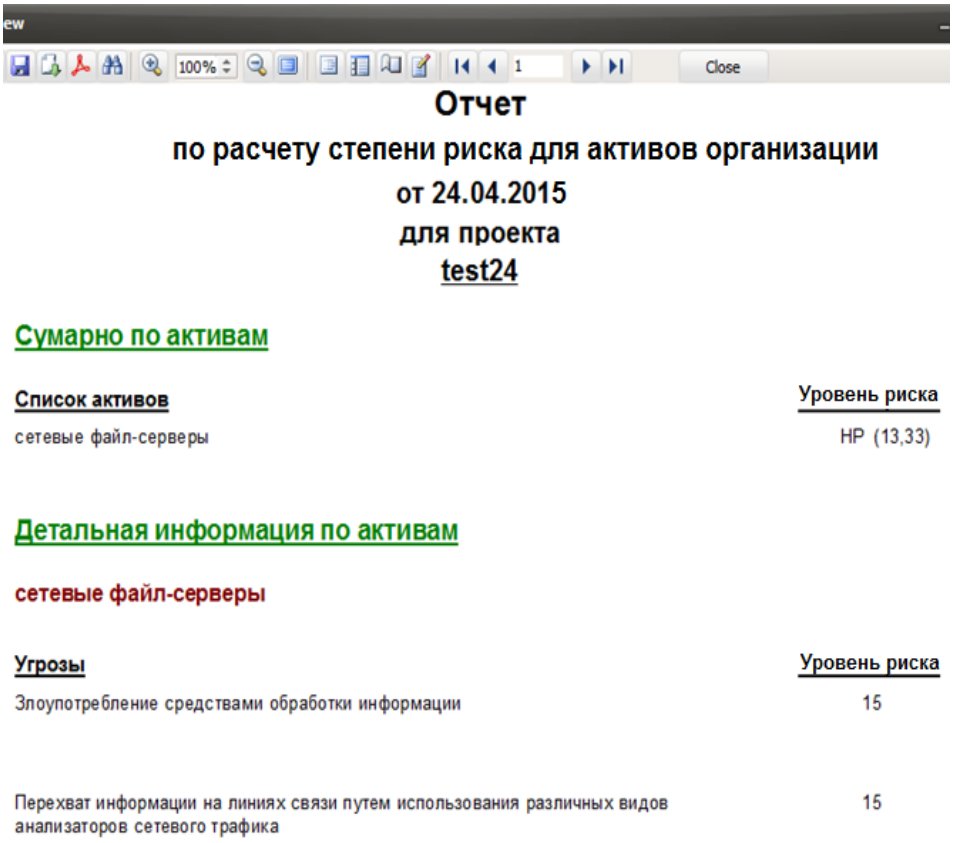
BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	12	1	0,37	0,01	15	ТҚ
BC_{12}	25	2	0,13	0,04	15	ТҚ
BC_{13}	5	2	0,05	0,03	10	ТҚ

Көріп отырғанымыздай, әрбір BC_{1bc_1} үшін $lr^{(BC_{1bc_1})}$ мәні «ақпараттық қауіпсіздік бұзылауында қатер деңгейі өте төмен» деңгейінде түсіндіріледі. IR_1 үшін шама $lr^{(cp)}$=13,33 болады, онда ЛА – ТҚ сәйкес келеді (4.6. сурет).

Берілген есептен $lr^{(BC_{1bc_1})}$мәнінің айтарлықтай төмендейтінін байқайға болады (4.6. сурет). Одан ПҚ First - ҚБАҚ жұмысы бағалау ортасының шартының өзгерісіне баланысты болады деген шешім шығаруға болады.

Екінші жағдайды ескеріп, қорғау нысанында алдыңғы бағалау нәтижелері ескерілмеген жағдайдағы үлгілеу жүзеге асыралады. Ақпараттық қауіпсіздік қатерлерді бағалау және талдауды алғашқы орындағаннан кейін алынған нәтижелер ескерелмеді және ақпараттық қауіпсіздік қамсыздандырулары енгізілмеді. Оның нәтижесінде қайта бағалағаннан кейін IR_1 таңдалған күй төмендеді. Ол сарапшылардың негізгі сипаттамалар мәндерді сарапшылар ұсынғандығы дәлелдейді (4.4-кесте). 4.4-кестеден көріп отырғанымыздай, $lr^{(BC_{1bc_1})}$ шамасы әрбір BC_{1bc_1} үшін айтарлықтай өседі, ал екі қатер үшін «ҚТ» «ҚО»-ке өзгереді. Бұл жағдайда ақпараттық қауіпсіздік бұзу қатерлер деңгейі орташа болады.

IR_1 үшін мәні $lr^{(cp)}$=43,33 болады, (4.1) өрнегіне сәйкес $\underset{\sim}{T}_{LR}$=«ҚО». Бұл қорғау нысаны үшін бірінші есептегі $lr^{(cp)}$ =31,67, $\underset{\sim}{T}_{LR}$=«ҚТ» салыстырғанда ақпараттық қауіпсіздік қатысты теріс үрдістер көрсетеді.



Отчет

по расчету степени риска для активов организации

от 24.04.2015

для проекта

test24

Сумарно по активам

Список активов	Уровень риска
сетевые файл-серверы	HP (13,33)

Детальная информация по активам

сетевые файл-серверы

Угрозы	Уровень риска
Злоупотребление средствами обработки информации	15
Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика	15

Сурет 4.6 – First – ҚБАҚ ПҚ $lr^{(BC_{1bc_1})}$ бағалау нәтижелері

Бірінші және екінші күйлерді есепке ала отырып, қосымша үш ақпараттық қауіпсіздік арналған қатерлерді бағалау жүргізілді. Аталмыш ақпараттық қауіпсіздіктің $lr^{(cp)}$ орташа мәнінің нәтижелері 4.5-кестеде және 4.7-суретте көрсетілген.

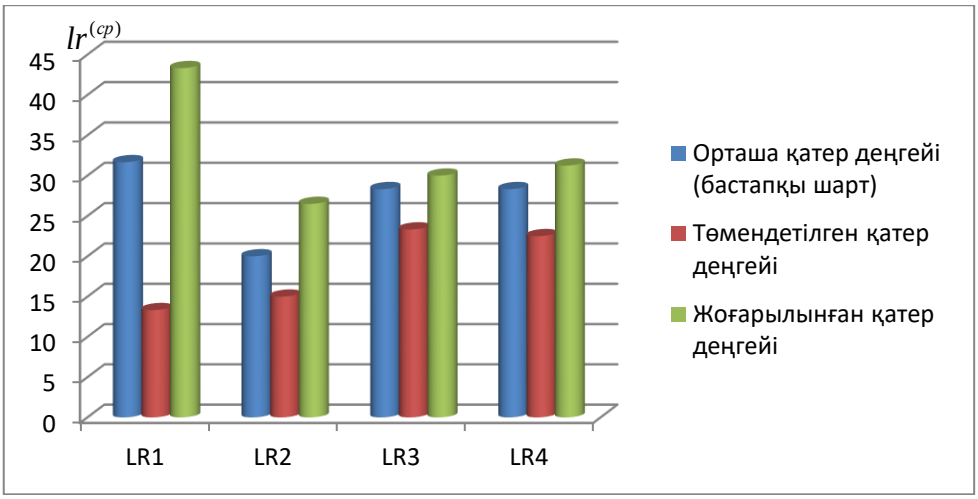
Кесте 4.4 - First - ҚБАҚ ПҚ бағалау нәтижелері

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	52	1	0,81	0,05	40	*ҚТ*
BC_{12}	45	4	0,23	0,31	45	*ҚО*
BC_{13}	43	3	0,47	0,27	45	*ҚО*

Алынып отырған нәтижелерді салыстыра отырып, негізгі сипаттамалар мәндерінің өзгерісінде құрылып отырған ПҚ First – ҚБАҚ бағалау ортасының шартына сәйкесінше әсер етеді деген шешімге келуге болады.

Кесте 4.5 - First – ҚБАҚ ПҚ $lr^{(cp)}$ мәндері

АҚ	$lr^{(cp)}$		
	Орташа қатер деңгейі (бастапқы шарт)	Төмендетілген қатер деңгейі	Жоғарылатынған қатер деңгейі
IR₁	31,67 (*ҚТ*)	13,33 (*ТҚ*)	43,33 (*ҚО*)
IR₂	20 (*ТҚ*)	15 (*ТҚ*)	26,5 (*ҚТ*)
IR₃	28,33 (*ҚТ*)	23,33 (*ҚТ*)	30 (*ҚТ*)
IR₄	28,33 (*ҚТ*)	22,5 (*ҚТ*)	31,25 (*ҚТ*)



Сурет 4.7 - First – ҚБАҚ ПҚ қатер деңгейлерінің орташа мәндер гистограммасы

Осыған ұқсас жолдармен алдыңғы тәжірибелермен өзге BC_{1bc_1} үшін қосымша зерттеулер жүргізілді. Жүргізілген зерттеу нәтижелері 4.6-4.8 кестелерінде келтірілді.

Кесте 4.6 - First – ҚБАҚ ПҚ бағалау нәтижелері

ҚОЖ	НС	BC_{11}	BC_{12}	BC_{13}	BC_{14}	$lr^{(cp)}$ $(\underset{\sim}{T}_{LR})$
1	2	3	4	5	6	7
1	***BC₃***	30	41	12	–	–
	BC₄	2	2	3	–	–
	BC₅	0,15	0,36	0,17	–	–
	BC₆	0,12	0,01	0,05	–	–
	$lr^{(BC_{1bc_1})}$ $(\underset{\sim}{T}_{LR})$	20 (*ТҚ*)	25 (ҚТ)	15 (ТҚ)	–	20 (ТҚ)
2	***BC₃***	30	41	12	16	–

	2	3	4	5	6	7
	BC_4	2	2	3	5	–
	BC_5	0,15	0,36	0,17	0,23	–
	BC_6	0,12	0,01	0,05	0,17	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	20 (ТҚ)	25 (ҚТ)	15 (ТҚ)	30 (ҚТ)	22,5 (ҚТ)
3	BC_3	23	23	9	–	–
	BC_4	2	1	1	–	–
	BC_5	0,07	0,3	0,06	–	–
	BC_6	0,03	0,01	0,05	–	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	15 (ТҚ)	20 (ТҚ)	10 (ТҚ)	–	15 (ТҚ)
4	BC_3	36	47	23	–	–
	BC_4	2	5	4	–	–
	BC_5	0,15	0,39	0,21	–	–
	BC_6	0,16	0,08	0,08	–	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	20 (ТҚ)	35 (ҚТ)	25 (ҚТ)	–	26,67 (ҚТ)
5	BC_3	32	23	47	–	–
	BC_4	4	2	3	–	–
	BC_5	0,21	0,12	0,2	–	–
	BC_6	0,3	0,03	0,06	–	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	40 (ҚТ)	15 (ТҚ)	30 (ҚТ)	–	28,33 (ҚТ)
6	BC_3	32	23	47	41	–
	BC_4	4	2	3	5	–
	BC_5	0,21	0,12	0,2	0,33	–
	BC_6	0,3	0,03	0,06	0,1	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	40 (ҚТ)	15 (ТҚ)	30 (ҚТ)	40 (ҚТ)	31,25 (ҚТ)
7	BC_3	26	17	22	–	–
	BC_4	3	1	3	–	–
	BC_5	0,16	0,12	0,2	–	–
	BC_6	0, 3	0,01	0,03	–	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	35 (ҚТ)	10 (ТҚ)	25 (ҚТ)	–	23,33 (ҚТ)
8	BC_3	38	31	52	–	–
	BC_4	4	2	4	–	–
	BC_5	0,27	0,16	0,25	–	–
	BC_6	0,33	0,04	0,12	–	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	40 (ҚТ)	15 (ҚТ)	35 (ҚТ)	–	30 (ҚТ)

4.6 - кестеде келесі қысқартулар қолданылған: ҚОЖ – қоршаған ортаның жағдайы, ол 1 мен 5 аралығында бастапқы шарттарды, 2 мен 6 – берілген ақпараттық қауіпсіздік қатерлер санының өзгерістерін, 3 мен 8 – бағаланушы

құраушы мәндерінің өзгерісін білдіреді (3 және 7 – негізгі сипаттамалар мәндерінің азаюы; 4 және 8 – негізгі сипаттамалар мәндерінің көбеюі); НС – негізгі сипаттамалар.

Тағы да жүргізілген көптеген зерттеу тәжірибелерінің нәтижелеріне тоқталып өтелік. Негізгі сипаттамаларды қолданудың салыстырмалы болжамын растау үшін осы сипаттамалардың әр түрлі жиынтығында ақпараттық қауіпсіздік қатерлерін бағалау және талдауды жүргізу керек (4.8. сурет). Зерттеу нәтижелері ПҚ First – ҚБАҚ түрлі бағалау ортасының шарттарында негізгі сипаттамалары мәндерінің өзгерісіне тікелей тіуелді болатынын және олардың негізінің өзгерісіне байланысты қатер мәнінің айтарлықтай өзгеретінін дәлелдеп берді.

Кесте 4.7- First – ҚБАҚ ПҚ BC_{13}

НС	BC_{13}	
BC₃	12	47
BC₄	3	3
BC₅	0,17	0,2
BC₆	0,05	0,06

Кесте 4.8 - First – ҚБАҚ ПҚ $lr^{(BC_{1bc_1})}$ мәндері

BC_{1bc_1}	$lr^{(BC_{1bc_1})}$ $(\underset{\sim}{T}_{LR})$	
BC_{11}	20 (ТҚ)	40 (ҚТ)
BC_{12}	25 (ҚТ)	15 (ТҚ)
$lr^{(cp)}$ $(\underset{\sim}{T}_{LR})$	22,5 (ҚТ)	27,5 (ҚТ)

Отчет
по расчету уровня риска для активов организации
от 22.06.2015
для проекта
Zero_Condition

Сумарно по активам

Список активов	Уровень риска
несетевые серверы общего назначения	HP - 16

Детальная информация по активам

несетевые серверы общего назначения

Угрозы	Уровень риска
Физический несанкционированный доступ в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	10
Кража или повреждение компьютерного оборудования и носителей информации инсайдерами	10
Кража или повреждение компьютерного оборудования и носителей информации внешними злоумышленниками	15
Постороннее лицо может получить физический доступ к комплексу средств защиты с целью переконфигурирования либо создания возможности обхода средств защиты	20
Кража бумажных документов инсайдерами	25

Сурет 4.8 - Бір негізгі сипаттаманы таңдаған кездегі First – ҚБАҚ ПҚ есебінің мысалы

4.3 Second – ҚБАҚ жүйесін зерттеу

Енді сенімсіз аймақта жұмыс жасайтын, яғни, сарапшы өзінің артықшылықтарына сенімсіздік танытқан кездегі Second – ҚБАҚ жүйесінің жұмысына тоқталып өтелік.

Келесі ҚД бағалау үшін 3.1 тараудағы әдістеме бойынша <*LR*, $\underset{\sim}{T}_{LR}$, X_{LR}> кортежіне сәйкес лингвистикалық айнымалыны (ЛА) «ҚАТЕР ДЕҢГЕЙІ» (*LR*) анықтау жүзеге асырылады. Ол үшін негізгі $\underset{\sim}{T}_{LR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{LR_j}$ ($j = \overline{1,m}$, мұндағы, m – термдер саны) терм-жиын анықталады. Егер *LR* үшін олар m болса, онда аралықтар саны G=2m-1 болады. Жалпы түрі [b_{11}; b_{21}[, [b_{21}; b_{12}[, [b_{12}; b_{22}[, …, [b_{2j-1}; b_{1j}[, [b_{1j}; b_{2j}[, …, [b_{2m-1}; b_{1m}[, [b_{1m}; b_{2m}] ($j = \overline{1,m}$), қатыстық функциялары (ҚФ) *μj(lr)* болады. $\underset{\sim}{T}_{LR_1}, \ldots, \underset{\sim}{T}_{LR_j}, \ldots, \underset{\sim}{T}_{LR_m}$ 2.4 тарауға сәйкес ҚФ-пен трапеция түріндегі анық емес сандарды (АЕС) $\mu_1(lr)$, …, $\mu_j(lr)$, …, $\mu_m(lr)$ береді. Олар төменде берілген (4.2) өрнегі бойынша есептеледі:

$$\mu_j(lr) = \begin{cases} L\left(\dfrac{b_{1j} - lr}{b_{1j} - a_j}\right), & lr \in [a_j, b_{1j}]; \\ 1, & lr \in [b_{1j}, b_{2j}]; \\ R\left(\dfrac{lr - b_{2j}}{c_j - b_{2j}}\right), & lr \in [b_{2j}, c_j], \end{cases} \qquad (4.2)$$

Мұндағы, $a_j < b_{1j} \le b_{2j} < c_j$, егер $j = \overline{1,m}$, $\{a_1\ c_m\} = \{\varnothing\}$ болса, *L(lr)*, *R(lr)*– функциялар (оң емес сандар жиынында өспейтін), *L(–lr)=L(lr)*, *R(–lr) = R(lr)*, *L(0) = R(0)* =1 қасиеттерін қанағаттандырады. Мысалы, m=5 болса, онда $\bigcup_{j=1}^{5} \underset{\sim}{T}_{LR_j}$ = {«Ақпараттық қауіпсіздік бұзу қатер деңгейі өте төмен» (*ТҚ*); «Ақпараттық қауіпсіздік бұзу қатер деңгейі төмен» (*ҚТ*); «Ақпараттық қауіпсіздік бұзу қатер деңгейі орташа» (*ҚО*); «Ақпараттық қауіпсіздік бұзу қатер деңгейі жоғары» (*ҚЖ*); «Ақпараттық қауіпсіздік бұзу қатер деңгейі өте жоғары» (*ЖҚ*)}. Олай болса, *G*=9, ал, (4.2) ескеріп, [b_{11}; b_{21}[,[b_{21}; b_{12}[,[b_{12}; b_{22}[,[b_{22}; b_{13}[,[b_{13}; b_{23}[,[b_{23}; b_{14}[,[b_{14}; b_{24}[, [b_{24}; b_{15}[,[b_{15}; b_{25}] аралықтарына [b_{11}; b_{21}[,[a_2, c_1[,[b_{12}; b_{22}[,[a_3; c_2[,[b_{13}; b_{23}[,[a_4; c_3[,[b_{14}; b_{24}[, [a_5; c_4[,[b_{15}; b_{25}] сәйкес болады. Ал, нақты мәліметтер мысал ретінде 4.9-кестеде берілген.

Лингвистикалық танып-білуге арналған алынған ҚД сандық мәніне $lr^{(BC_{1bc_1})}$ құрылымдық ҚД SP параметрлерді қалыптастыруда (4.2) формула қолданылады:

$$SP^{(BC_{1bc_1})} = \begin{cases} (lr^{(BC_{1bc_1})}; \underset{\sim}{T}_{LR_j}) \; егер \; \mu_j(lr) = 1; \\ (lr^{(BC_{1bc_1})}; \underset{\sim}{T}_{LR_j}(\mu_j(lr)); \underset{\sim}{T}_{LR_{j+1}}(\mu_{j+1}(lr))) \; егер \; \mu_j(lr), \mu_{j+1}(lr) \neq 1, \end{cases} \quad (4.3)$$

Мұндағы $(lr^{(BC_{1bc_1})}; \underset{\sim}{T}_{LR_j})$ сандық $lr^{(BC_{1bc_1})}$ теңдікті $\underset{\sim}{T}_{LR_j}$ қатердің деңгейі сияқты ауызша түсіндіріледі. Ал, $(lr^{(BC_{1bc_1})}; \underset{\sim}{T}_{LR_j}(\mu_j(lr)); \underset{\sim}{T}_{LR_{j+1}}(\mu_{j+1}(lr)))$ болса, $\underset{\sim}{T}_{LR_j}$ – $\mu_j(lr)$ және $\underset{\sim}{T}_{LR_{j+1}}$ – $\mu_{j+1}(lr)$ аралығында сарапшының сенімділігімен $\underset{\sim}{T}_{LR_j}$ және $\underset{\sim}{T}_{LR_{j+1}}$ аралығындағы мәндерді қабылдай алатын сандық $lr^{(BC_{1bc_1})}$ теңдікті ҚД сияқты ауызша түсіндіріледі.

Кесте 4.9 - Second – ҚБАҚ ПҚ аралық мәндерінің және $\mu_j(lr)$ мысалы

Аралығы	Термдер	$\mu_j(lr)$
$[b_{11}; b_{21}[=[0; 10[$	$\underset{\sim}{T}_{LR_1}$	1
$[b_{21}; b_{12}[=[10; 20[$	$\underset{\sim}{T}_{LR_1}$	$\mu_1(lr)=(20-lr)/10$
	$\underset{\sim}{T}_{LR_2}$	$\mu_2(lr)=1-\mu_1(lr)$
$[b_{12}; b_{22}[=[20; 30[$	$\underset{\sim}{T}_{LR_2}$	1
$[b_{22}; b_{13}[=[30; 40[$	$\underset{\sim}{T}_{LR_2}$	$\mu_2(lr)=(40-lr)/10$
	$\underset{\sim}{T}_{LR_3}$	$\mu_3(lr)=1-\mu_2(lr)$
$[b_{13}; b_{23}[=[40; 50[$	$\underset{\sim}{T}_{LR_3}$	1
$[b_{23}; b_{14}[=[50; 60[$	$\underset{\sim}{T}_{LR_3}$	$\mu_3(lr)=(60-lr)/10$
	$\underset{\sim}{T}_{LR_4}$	$\mu_4(lr)=1-\mu_3(lr)$
$[b_{14}; b_{24}[=[60; 70[$	$\underset{\sim}{T}_{LR_4}$	1
$[b_{24}; b_{15}[=[70; 80[$	$\underset{\sim}{T}_{LR_4}$	$\mu_4(lr)=(80-lr)/10$
	$\underset{\sim}{T}_{LR_5}$	$\mu_5(lr)=1-\mu_4(lr)$
$[b_{15}; b_{25}]=[80; 100]$	$\underset{\sim}{T}_{LR_5}$	1

ПҚ–ның НС эталондық мәнін қалыптастыру кезеңінде ЛА «EC_i ДЕҢГЕЙІ» (C_{EC_i}) қалыптасады. Ол 2.4 тарауда қарастырылған $<C_{EC_i}, \underset{\sim}{T}_{C_{EC_i}}, X_{EC_i}>$ кортежбен анықталады. Мұнда негізгі терм-жиыны m термімен $\underset{\sim}{T}_{C_{EC_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{C_{EC_i j}}$ беріледі. Мысалы, m=5 болған кездегі жағдайлар 4.10-кестеде берілген.

Кесте 4.10 - $\mu_j(ec_i^{BC_{1bc_1}})$ ($i=\overline{1,4}$, $j=\overline{1,5}$) және аралық мәндерінің мысалы

EC_i үшін аралықтар				Термдер	$\mu_j(ec_i^{BC_{1bc_1}})$			
BC₃	***BC₄***	***BC₅***	***BC₆***	$\underset{\sim}{T}_{C_{EC_i j}}$	$\mu_j(ec_1^{BC_{1bc_1}})$	$\mu_j(ec_2^{BC_{1bc_1}})$	$\mu_j(ec_3^{BC_{1bc_1}})$	$\mu_j(ec_4^{BC_{1bc_1}})$
[0;10[	[0;1[	[0;0,1[	[0;0,1[	$\underset{\sim}{T}_{C_{EC_i 1}}$	$\mu_1(ec_1^{BC_{1bc_1}})=1$	$\mu_1(ec_4^{BC_{1bc_1}})=1$	$\mu_1(ec_3^{BC_{1bc_1}})=1$	$\mu_1(ec_4^{BC_{1bc_1}})=1$
[10;20[	[1;2[	[0,1;0,2[	[0,1;0,15[	$\underset{\sim}{T}_{C_{EC_i 1}}$	$\mu_1(ec_1^{BC_{1bc_1}})=(20-ec_1^{BC_{1bc_1}})/10$	$\mu_1(ec_2^{BC_{1bc_1}})=(2-ec_2^{BC_{1bc_1}})$	$\mu_1(ec_3^{BC_{1bc_1}})=(0,2-ec_3^{BC_{1bc_1}})*10$	$\mu_1(ec_4^{BC_{1bc_1}})=(0,15-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i 2}}$	$\mu_2(ec_1^{BC_{1bc_1}})=1-\mu_1(ec_1^{BC_{1bc_1}})$	$\mu_2(ec_2^{BC_{1bc_1}})=1-\mu_1(ec_2^{BC_{1bc_1}})$	$\mu_2(ec_3^{BC_{1bc_1}})=1-\mu_1(ec_3^{BC_{1bc_1}})$	$\mu_2(ec_4^{BC_{1bc_1}})=1-\mu_1(ec_4^{BC_{1bc_1}})$
[20;30[	[2;3[	[0,2;0,3[	[0,15;0,2[	$\underset{\sim}{T}_{C_{EC_i 2}}$	$\mu_2(ec_1^{BC_{1bc_1}})=1$	$\mu_2(ec_2^{BC_{1bc_1}})=1$	$\mu_2(ec_3^{BC_{1bc_1}})=1$	$\mu_2(ec_4^{BC_{1bc_1}})=1$
[30;40[	[3;4[	[0,3;0,4[	[0,2;0,25[	$\underset{\sim}{T}_{C_{EC_i 2}}$	$\mu_2(ec_1^{BC_{1bc_1}})=(40-ec_1^{BC_{1bc_1}})/10$	$\mu_2(ec_2^{BC_{1bc_1}})=(4-ec_2^{BC_{1bc_1}})$	$\mu_2(ec_3^{BC_{1bc_1}})=(0,4-ec_3^{BC_{1bc_1}})*10$	$\mu_2(ec_4^{BC_{1bc_1}})=(0,25-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i 3}}$	$\mu_3(ec_1^{BC_{1bc_1}})=1-\mu_2(ec_1^{BC_{1bc_1}})$	$\mu_3(ec_2^{BC_{1bc_1}})=1-\mu_2(ec_2^{BC_{1bc_1}})$	$\mu_3(ec_3^{BC_{1bc_1}})=1-\mu_2(ec_3^{BC_{1bc_1}})$	$\mu_3(ec_4^{BC_{1bc_1}})=1-\mu_2(ec_4^{BC_{1bc_1}})$
[40;50[	[4;5[	[0,4;0,5[	[0,25;0,3[	$\underset{\sim}{T}_{C_{EC_i 3}}$	$\mu_3(ec_1^{BC_{1bc_1}})=1$	$\mu_3(ec_2^{BC_{1bc_1}})=1$	$\mu_3(ec_3^{BC_{1bc_1}})=1$	$\mu_3(ec_4^{BC_{1bc_1}})=1$

1	2	3	4	5	6	7	8	9
[50;60[	[5;6[	[0,5;0,6[	[0,3;0,35[	$\underset{\sim}{T}_{C_{EC_i}3}$	$\mu_3(ec_1^{BC_{1bc_1}})=(60-ec_1^{BC_{1bc_1}})/10$	$\mu_3(ec_2^{BC_{1bc_1}})=(6-ec_2^{BC_{1bc_1}})$	$\mu_3(ec_3^{BC_{1bc_1}})=(0,6-ec_3^{BC_{1bc_1}})*10$	$\mu_3(ec_3^{BC_{1bc_1}})=(0,35-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i}4}$	$\mu_4(ec_1^{BC_{1bc_1}})=1-\mu_3(ec_1^{BC_{1bc_1}})$	$\mu_4(ec_2^{BC_{1bc_1}})=1-\mu_3(ec_2^{BC_{1bc_1}})$	$\mu_4(ec_3^{BC_{1bc_1}})=1-\mu_3(ec_3^{BC_{1bc_1}})$	$\mu_4(ec_4^{BC_{1bc_1}})=1-\mu_3(ec_4^{BC_{1bc_1}})$
[60;70[	[6;7[	[0,6;0,7[	[0,35;0,4[	$\underset{\sim}{T}_{C_{EC_i}4}$	$\mu_4(ec_1^{BC_{1bc_1}})=1$	$\mu_4(ec_2^{BC_{1bc_1}})=1$	$\mu_4(ec_3^{BC_{1bc_1}})=1$	$\mu_4(ec_4^{BC_{1bc_1}})=1$
[70;80[	[7;8[	[0,7;0,8[	[0,4;0,45[	$\underset{\sim}{T}_{C_{EC_i}4}$	$\mu_4(ec_1^{BC_{1bc_1}})=(80-ec_1^{BC_{1bc_1}})/10$	$\mu_4(ec_2^{BC_{1bc_1}})=(8-ec_2^{BC_{1bc_1}})$	$\mu_4(ec_3^{BC_{1bc_1}})=(0,8-ec_3^{BC_{1bc_1}})*10$	$\mu_4(ec_4^{BC_{1bc_1}})=(0,45-ec_4^{BC_{1bc_1}})*20$
				$\underset{\sim}{T}_{C_{EC_i}5}$	$\mu_5(ec_1^{BC_{1bc_1}})=1-\mu_4(ec_1^{BC_{1bc_1}})$	$\mu_5(ec_2^{BC_{1bc_1}})=1-\mu_4(ec_2^{BC_{1bc_1}})$	$\mu_5(ec_3^{BC_{1bc_1}})=1-\mu_4(ec_3^{BC_{1bc_1}})$	$\mu_5(ec_4^{BC_{1bc_1}})=1-\mu_4(ec_4^{BC_{1bc_1}})$
[80;100]	[8;10[	[0,8;1[	[0,45;0,5[	$\underset{\sim}{T}_{C_{EC_i}5}$	$\mu_5(ec_1^{BC_{1bc_1}})=1$	$\mu_5(ec_2^{BC_{1bc_1}})=1$	$\mu_5(ec_3^{BC_{1bc_1}})=1$	$\mu_5(ec_4^{BC_{1bc_1}})=1$

ПС-тағы ҚД бағалау және ағымдық мәндерді жіктеу автоматтандырылған режимде жүзеге асырылады. Әрбір қатер әрекеті үшін $lr^{(BC_{1bc_1})}$ мәні ПҚ First – ҚБАҚ сипатының өрнегіне сәйкес есептелінеді, бірақ, айырмашылығы $\lambda_{ij}^{(BC_{1bc_1})}$ мәні төмендегі формула бойынша анықталады:

$$\lambda_{i1}^{(BC_{1bc_1})}=\begin{cases}1\ егер\ ec_i^{BC_{1bc_1}}\in[bi_{11},bi_{12}[;\\ 0\ егер\ ec_i^{BC_{1bc_1}}\notin[bi_{11},ci_1[;\\ \mu_1(ec_i^{BC_{1bc_1}})\ егер\ ec_i^{BC_{1bc_1}}\in[bi_{12},ci_1[,\end{cases}$$

$$\lambda_{ij}^{(BC_{1bc_1})}=\begin{cases}\mu_j(ec_i^{BC_{1bc_1}})\ егер\ ec_i^{BC_{1bc_1}}\in[ai_j,bi_{1j}[;\\ 1\ егер\ ec_i^{BC_{1bc_1}}\in[bi_{1j},bi_{2j}[;\\ \mu_j(ec_i^{BC_{1bc_1}})\ егер\ ec_i^{BC_{1bc_1}}\in[bi_{2j},ci_j[;\\ 0\ егер\ ec_i^{BC_{1bc_1}}\notin[ai_j,ci_j[,\end{cases}$$

$$\lambda_{im}^{(BC_{1bc_1})} = \begin{cases} \mu_m(ec_i^{BC_{1bc_1}}) \text{ егер } ec_i^{BC_{1bc_1}} \in [ai_m, bi_{1m}[; \\ 1 \text{ егер } ec_i^{BC_{1bc_1}} \in [bi_{1m}, bi_{2m}[; \\ 0 \text{ егер } ec_i^{BC_{1bc_1}} \notin [ai_m, bi_{2m}[, \end{cases}$$

$(j=\overline{2,m-1}),\ (i=\overline{1,g})$.

АҚ үшін $lr^{(cp)}$ мәні First – ҚБАҚ жүйесіндігідей есептеледі.

Алынған нәтижелер өңделіп, түсіндіріліп, есеп түрінде беріледі.

Негізгі функцияларды тексеру үшін және ПҚ Second – ҚБАҚ жұмыс жасау принципін бейнелеу мақсатында оларды тексеру жүргізіледі. Жүйе жұмысының алынған нәтижелерін салыстыру First – ҚБАҚ жүйесіндегідей IR_1–де орнатылған BC_{1bc_1} негізделеді. Тестілеу берілген лигвистикалық түрдегі нақты бастапқы мәліметтерге арналып жүргізілді. Одан соң әрбір қатер бойынша $lr^{(BC_{1bc_1})}$ мәнін есептеу жүргізіледі. Оның нәтижелері 4.11-кестесіне енгізілді. Беріліп отырған 4.11-кестесінен ақпараттық қауіпсіздік үшін ҚД мәні барлық қатерлерде төмен екендігін байқауымызға болады.

Кесте 4.11- Second – ҚБАҚ ПҚ негізгі сипаттамаларының және $lr^{(BC_{1bc_1})}$ мәндері

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	42	1	0,67	0,05	35	*ҚТ*
BC_{12}	25	4	0,13	0,31	37,5	*ҚТ*
BC_{13}	33	3	0,07	0,17	30	*ҚТ*

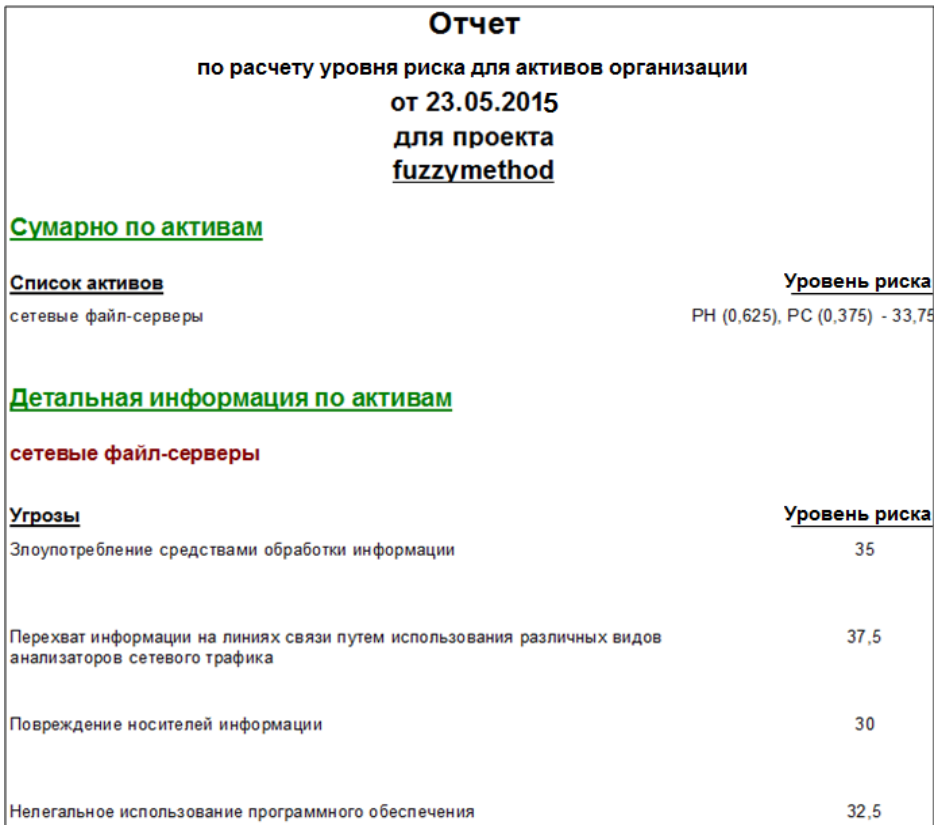
Одан кейін IR_1 үшін $lr^{(cp)}$=34,17 орташа мәнін есептеу жүргізіледі. (4.3) өрнегі лингвистикалық түсіндіруге сәйкес келеді: 34,17 сандық мәні бар ҚД төменгі және орташа қатерлер аралығында, ал, сарапшы сенімділігі ҚТ – 0,58 және ҚО – 0,42 аралығында болады.

Одан кейінгі ПҚ тексеру First – ҚБАҚ жүйесіне сәйкес бағалау ортасының бірнеше күйлерін үлгілеу негізінде жүргізілді: 1-ші күй – Ақпараттық қауіпсіздік үшін қатерлер санын орнатумен байланысты алғашқы шарттар; 2-ші күй – Ақпараттық қауіпсіздік үшін қатерлер санының көбеюі; 3-ші күй – Ақпараттық қауіпсіздік үшін бір қатерді бұғаттау; 4-ші күй – негізгі сипаттамалар мәндерінің өзгеруі (азаюы немесе көбеюі).

1-ші күй алғашқы шарттарды және ҚД есептеу нәтижелерін қамтиды. Ол 4.11-кестеде берілді.

2–ші күй. Бағалау нысанында қоршаған орта шарттары өзгерді. Оның нәтижесінде BC_{14} үшін ҚД мәнін есептеу жүргізілді, $lr^{(BC_{14})}$=32,5. Ал $lr^{(cp)}$ мәні BC_{14} енгізгеннен кейін $lr^{(cp)}$= 33,75 (ҚТ (0,625), ҚО (0,375)) тең болды. Ал мән енгізгеннен кейін төменгі (сарапшының сенімділігі 0,625) және орташа

(сарапшының сенімділігі 0,375) қатерлер мәндерінің аралығында болды (4.9. сурет).



Отчет

по расчету уровня риска для активов организации
от 23.05.2015
для проекта
fuzzymethod

Сумарно по активам

Список активов	Уровень риска
сетевые файл-серверы	PH (0,625), PC (0,375) - 33,75

Детальная информация по активам

сетевые файл-серверы

Угрозы	Уровень риска
Злоупотребление средствами обработки информации	35
Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика	37,5
Повреждение носителей информации	30
Нелегальное использование программного обеспечения	32,5

Сурет 4.9 - Second – ҚБАҚ ПҚ ақпараттық қауіпсіздік мәндері есебінің терезесі

3–ші күй. Одан кейін BC_{12}=«Желілік трафикті талдаулардың әр түрлі түрлерін қолдану арқылы байланыс желілерінде ақпараттарды жібермеу» болдырмауға байланысты жасалатын нысанды қорғауды бағалауда үлгілеу жүргізілді. Сонымен қатар $lr^{(BC_{1bc_1})}$ және $lr^{(cp)}$ қайта есептелінді. Үлгіленетін жағдайларды ескере отырып құрылған жүйені қолданып, IR_1 үшін $lr^{(cp)}$ алынған мәні 32,5 (ҚТ (0,75), ҚО (0,25)) дейін азайды, яғни, $lr^{(cp)}$ төменгі (сарапшының сенімділігі 0,75) және орташа (сарапшының сенімділігі 0,25) қатерлер мәндерінің аралығында болады. Мұнда $lr^{(cp)}$ мәні BC_{1bc_1} саны өзгерген кезде өзгереді. Одан әрі жүргізілген тәжірибе нәтижелері BC_{1bc_1} санының айтарлықтай көбейгенінде немесе азайғанында $lr^{(cp)}$ мәні де сәйкесінше өзгеретіндігін көрсетіп берді.

4–ші күй. Есептеулерді жүргізіп болғаннан кейін 1-ші күйге сәйкес екі жағдай үшін үлгілеу жүргізілді:

– біріншісінде қорғау нысанында ақпараттық қауіпсіздік қатерлерді бағалау және талдаудың алдыңғы нәтижелері ескерілді;

– екіншісінде қорғау нысанында бағалаудың алдыңғы нәтижелері ескерілмейді және қатерлерді азайту үшін оларды енгізуді жүзеге асыратын шешімдер қабылданбайды.

BC_{11}, BC_{12}, BC_{13} қатер деңгейлерін азайту мақсатында бағалай нысандарында түрлі іс-әрекеттер жүргізілді.

Ақпараттық қауіпсіздік қатерлерді бағалау және талдауды қайта жүзеге асырғаннан кейінгі сарапшылардың орнатқан негізгі сипаттамалар шамаларының мәндері 4.12-кестеде беріліп отыр.

Кесте 4.12 - Second – ҚБАҚ ПҚ негізгі құраушылары және $lr^{(BC_{1bc_1})}$ мәндері

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	12	1	0,37	0,01	23,5	ҚТ
BC_{12}	25	2	0,13	0,04	21,5	ҚТ
BC_{13}	5	2	0,05	0,03	15	ТҚ

Әрбір BC_{1bc_1} үшін $lr^{(BC_{1bc_1})}$ есептеу қайта жүргізілді (4.12-кесте). Олардың әрбірі IR_1 үшін $lr^{(cp)}$ шамасы есептелді $lr^{(cp)}$=20, $\underset{\sim}{T}_{LR}$ = «ҚТ» (сарапшының сенімділігі – 1) мәніне сәйкес келеді. Араластырылған ПҚ есебінен қатерлердің деңгейі азайғандығын көруге болады, соған байланысты ендірілген ақпараттық қауіпсіздік қамтамасыз ету тиімді болып табылады, ал, Second – ҚБАҚ жүйесі бағалау ортасының шарттарына тәуелді байланыста болып шықты.

Екінші жағдайды ескере отырып, бағалаудың алдыңғы нәтижелері есепке алынбағын үлгілеу жүргізілген. Бірінші бағалау жасалғаннан кейін алынған нәтижелер ескерілмеді және ақпараттық қауіпсіздік қамсыздандыру ендірілмеді.

Таңдалған ақпараттық қауіпсіздік үшін олардағы қатерлерді қайта бағалау және талдаудан кейін жағдай төмендеп кетті. Ол сарапшылардың негізгі сипаттамалар мәндерінің анықталғандығын көрсетеді (4.13-кесте). 4.13-кестеден $lr^{(BC_{1bc_1})}$ өскендігін және екі қатер үшін «ҚТ» мәнінің «ҚО» мәніне өзгергендігін көруге болады.

Кесте 4.13 - Second – ҚБАҚ ПҚ бағалау нәтижелері

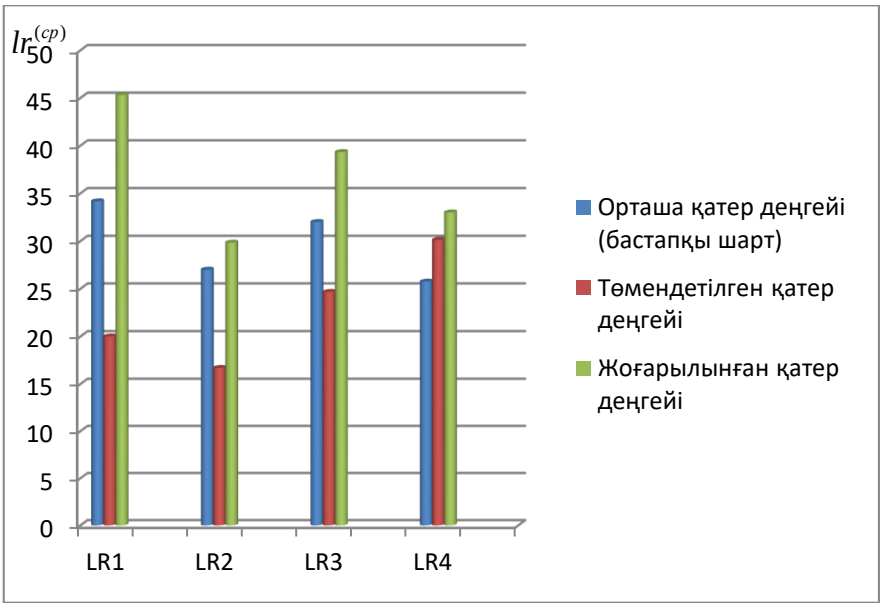
BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	52	1	0,81	0,05	45	*ҚТ*
BC_{12}	45	4	0,23	0,31	46	*ҚО*
BC_{13}	43	3	0,47	0,27	45	*ҚО*

IR_1 арналған $lr^{(cp)}$ шамасы $lr^{(cp)}$=45,33 тең, әрі $\underset{\sim}{T}_{LR}$ = «ҚО» мәніне сәйкес (сарапшы сенімділігі – 1) болады.

Бірінші және екінші күйлерді есепке ала отырып, қосымша үш ақпараттық қауіпсіздік арналған қатерлерді бағалау мен талдау жүргізіледі. 4.14-кестеде және 4.10. суретте осы ақпараттық қауіпсіздік арналған $lr^{(cp)}$ мәндері берілген.

Кесте 4.14 - Second – ҚБАҚ ПҚ $lr^{(cp)}$ мәндері

Ақпараттық қауіпсіздік	$lr^{(cp)}$		
	Орташа қатер деңгейі (бастапқы шарт)	Төмендетілген қатер деңгейі	Жоғарылатынған қатер деңгейі
IR1	34,17 (ҚТ (0,58), ҚО (0,42))	20 (ҚТ)	45,33 (ҚО)
IR2	2,7 (ҚТ)	16,7 (ТҚ (0,33), ҚТ (0,67))	29,83 (ҚТ)
IR3	32 (ҚТ (0,8), ҚО (0,2))	24,67 (ҚТ)	39,33 (ҚТ (0,07), ҚО (0,93))
IR4	25,75 (ҚТ)	30,13 (ҚТ (0,99), ҚО (0,01))	33 (ҚТ (0,70), ҚО (0,30))



Сурет 4.10 - Second – ҚБАҚ ПҚ қатер деңгейлерінің орташа мәндер гистограммасы

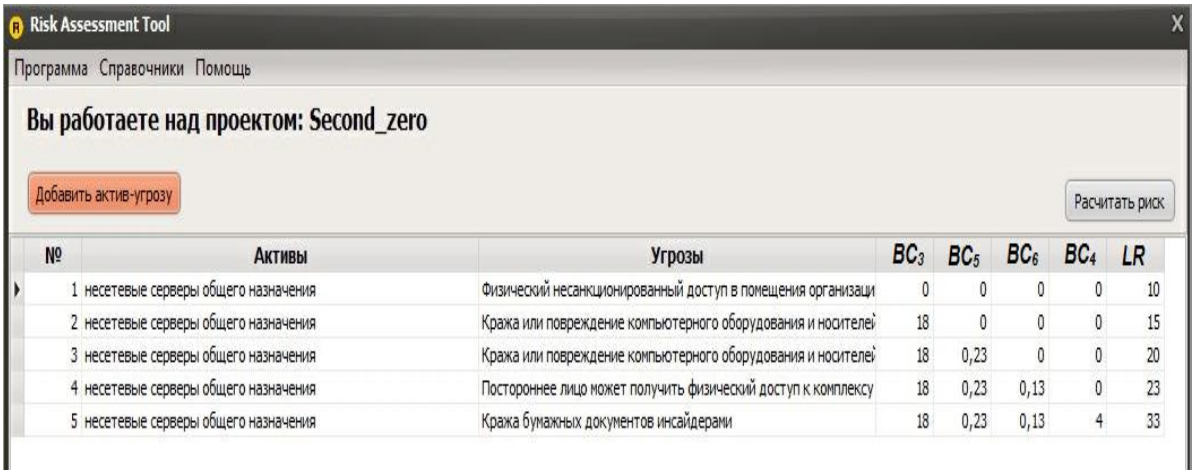
Алдыңғы қарастырылған тәжірибедегідей өзге BC_{1bc_1} үшін қосымша зерттеулер жүргізілді. Олардың нәтижелері 4.11-суретте беріліп және 4.15-кестеге енгізілді.

Кесте 4.15 - Second – ҚБАҚ ПҚ бағалау нәтижелері

ССО	НС	BC_{11}	BC_{12}	BC_{13}	**BC_{14}**	$lr^{(cp)}$ $(\underset{\sim}{T}_{LR})$
1	***BC₃***	30	41	12	–	–
	BC₄	2	2	3	–	–
	BC₅	0,15	0,36	0,17	–	–
	BC₆	0,12	0,01	0,05	–	–
	$lr^{(BC_{1bc_1})}$ $(\underset{\sim}{T}_{LR})$	24,5 (ҚТ)	33 (ҚТ)	23,5 (ҚТ)	–	27 (ҚТ)
2	***BC₃***	30	41	12	16	–
	BC₄	2	2	3	5	–
	BC₅	0,15	0,36	0,17	0,23	–
	BC₆	0,12	0,01	0,05	0,17	–
	$lr^{(BC_{1bc_1})}$ $(\underset{\sim}{T}_{LR})$	24,5 (ҚТ)	33 (ҚТ)	23,5 (ҚТ)	22,5 (ҚТ)	25,88 (ҚТ)
3	***BC₃***	23	23	9	–	–
	BC₄	2	1	1	–	–
	BC₅	0,07	0,3	0,06	–	–
	BC₆	0,03	0,01	0,05	–	–
	$lr^{(BC_{1bc_1})}$ $(\underset{\sim}{T}_{LR})$	20 (ТҚ)	20 (ТҚ)	10 (ТҚ)	–	16,67 – ТҚ (0,33), ҚТ (0,67)
4	***BC₃***	36	47	23	–	–
	BC₄	2	5	4	–	–
	BC₅	0,15	0,39	0,21	–	–
	BC₆	0,16	0,08	0,08	–	–
	$lr^{(BC_{1bc_1})}$ $(\underset{\sim}{T}_{LR})$	32,5 (ҚТ)	27 (ҚТ)	30 (ҚТ)	–	29,83 (ҚТ)
5	***BC₃***	32	23	47	–	–
	BC₄	4	2	3	–	–
	BC₅	0,21	0,12	0,2	–	–
	BC₆	0,3	0,03	0,06	–	–
	$lr^{(BC_{1bc_1})}$ $(\underset{\sim}{T}_{LR})$	45 (ҚО)	21 (ҚТ)	30 (ҚТ)	–	32 – ҚТ (0,8), ҚО (0,2)
6	***BC₃***	32	23	47	41	–
	BC₄	4	2	3	5	–

	2	3	4	5	6	7
	BC_5	0,21	0,12	0,2	0,33	–
	BC_6	0,3	0,03	0,06	0,1	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	45 (ҚО)	21 (ҚТ)	30 (ҚТ)	24,5 (ҚТ)	30,13 – ҚТ (0,99), ҚО (0,01)
7	BC_3	26	17	22	–	–
	BC_4	3	1	3	–	–
	BC_5	0,16	0,12	0,2	–	–
	BC_6	0, 3	0,01	0,03	–	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	33 (ҚТ)	16 (ҚТ)	25 (ҚТ)	–	24,67 (ҚТ)
8	BC_3	38	31	52	–	–
	BC_4	4	2	4	–	–
	BC_5	0,27	0,16	0,25	–	–
	BC_6	0,33	0,04	0,12	–	–
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	48 (ҚО)	28 (ҚТ)	42 (ҚО)	–	39,33 – ҚТ (0,07), ҚО (0,93)

Алынған зерттеу нәтижелері ПҚ Second – ҚБАҚ түрлі бағалау ортасы шартында таңдалған сипаттамалар негізінің мәндерінің өзгерісіне тепе тең әсер ететіндігін және қатердің мәні сәйкес негіздің өзгерісінде ешқандай өзгеріске ұшырамайтындығын анықтап берді.



Сурет 4.11 - Second – ҚБАҚ ПҚ әртүрлі негізгі сипаттамаларын таңдауға арналған жүйе терезесі

First-ҚБАҚ және Second-ҚБАҚ бағалау нәтижелерінен көріп отырғанымыздай жүйе бағалау ортасының өзгерісіне сәйкес жүргізіледі және кіріс шамаларында салыстырмалы нәтижелер береді.

Төртінші бөлім бойынша тұжырым

1. Зерттеу жұмысында дайындалған әдістер мен үлгілерді, ПҚ және құрылымдық шешімдерді тексеру мақсатында ПҚ ҚБАҚ бойынша тәжірибелік зерттеулер жүргізілді. ҚБАҚ тәжірибелік зерттеулері кез келген сипаттама негізінде тепе тең бағалауды жүзеге асыруға мүмкіндік беретіндігін көрсетіп берді. Сонымен қатар, әр түрлі бағалау ортасы шартына байланысты есептеулер жүргізілді: бастапқы кезеңде қорғау нысанының күйін; қатердің азаюына байланысты жүзеге асырылуын; қорғау жүйесінің болмау жағдайын. Ұсынылып отырған жүйелер шарттардың өзгерісіне тепе тең жауап береді.

2. Зерттеу жұмысында көрсетіліп отырған зерттеулерді енгізу және практикада қолдану нәтижесінде диссертациялық жұмыстың ғылыми қорытындылары мен теориялық болжамдарының анықтылығы мен дұрыстығын растайды.

ҚОРЫТЫНДЫ

Диссертациялық жұмыста ұсынылып отырған синтез әдістемесіне негізделген, қатердің ҚКМ әдісі және үлгісі бойынша жасалған тиімді ҚБАҚ ақпараттық қауіпсіздік құруда қолданылатын өзекті болып саналатын ғылыми зерттеулер жүргізіліп, шешімдерін тапты.

Қойылған мәселелерді шешу кезінде келесі ғылыми нәтижелер алынды:

1. Жүргізілген ҚБАҚ талдауы және оның негізгі түсініктері негізінде қатердің негізгі сипаттамаларының кортеждік үлгісі жасалды. Олар алты құрауышты кортежде бейнеленген негізгі сипаттамаларын қорытындылап, икемділікті қамтамасыз ететін және жасалған САОР қызметіне қажетті мәліметтер жиындарын қалыптастыруға мүмкіндік жасайды.

2. ҚКМ қорытынды үлгілерін және логикалық-лингвистикалық тәсілді қолдану негізінде ұсынылып отырған мүмкіндіктері өте жоғары ақпараттық қауіпсіздік қатерлерін бағалау және талдау әдістері бағалаудың қажетті құралдарын құруға мүмкіндік береді. Онда кіріс мәліметтері ретінде уақыт аралығын, саласын, нысанның экономикалық және әкімшілік т.б. ерекшеліктерін ескере отырып, анықталған және анық емес негізгі сипаттамалардың динамикалық өзгермелі жиынтығын қолданады.

3. Мәліметтер қорының қолдана отырып, термдер санын арттырудың n–еселі функциясын жүзеге асыратын әдістер жасалды. Оның көмегімен термдер санын бір ретке арттыруда n–еселі функцияны кеңейтуді түрлендіру арқылы эталондық ЛА термдер санының n есеге сәйкес түрлену үрдісін қалыптастыру мүмкіндіктері артады.

4. Зерттеу тақырыбында берілген ақпараттық қауіпсіздік қатерлерін бағалау және талдауда берілген жиын шамаларын пайдалану арқылы икемділік мүмкіндіктерге ие құралдарды қолдануды анықтайтын әдістер мен қалыптастырылған сипаттамалар үлгілерін қолдану үрдісін дайындау және қорытындылау негізінде ҚБАҚ синтездеу әдістемесінің одан әрі дамуы шешімін тапты.

5. Негізгі сипаттамаларды және анықталған мәліметтерді өңдеуші ішкі жүйелері көмегімен FirstM және SecondM әдістерін жүзеге асыратын ҚБАҚ жүйесінің құрылымы жасалды. Ол сандық және сапалық анықтауда мәліметтерді қалыптастыруға және түрлендіруге мүмкіндік береді.

6. Мәліметтер қоры негізінде ұсынылған әдістеме мен құрылымдық шешімдерде ҚБАҚ ақпараттық қауіпсіздік қолданбалы бағдарламасы жасалды. Онда түрлі сипаттамалар жиынтығының динамикалық өзгерісінің мүмкіндіктері есебінен анықталған және анық емес нашар байланысқан орталарда мәселені тиімді шешуді жүзеге асыру қолайлылық және икемділік қызметінің мүмкіндіктері көбейді.

7. Ұсынылған үлгілер, құрылған әдістер мен құрылымдық шешімдерді тексеру мақсатында ҚБАҚ бойынша тәжірибелер жүргізілді. Оларды практикалық қолданысқа енгізу диссертациялық жұмыстың қорытындылары

мен теориялық тұжырымдарының дұрыстығын және нақтылығын дәлелдеп берді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Алексеев А. Управление рисками. Метод CRAMM IT Expert. – Электрон. дан. – М. : ЗАО «ИТ Эксперт», 2010 //World Wide Web. – URL: http://www.itexpert.ru/rus/ ITEMS/ ITEMS_CRAMM.pdf. – Загл. с экрана (просмотрено 19 декабря 2014).

2 Төкеев У.А., Ахметов Б.Б. Ақпараттық қауіпсіздікті басқару: оқу құралы. – Алматы: әл-Фараби атындағы Қазақ ұлттық университеті, 2011. – 161 б.

3 Захаров А.И. Информационные системы: оценка рисков //Information Security (Информационная безопасность) – 2005. – №6 – С. 18–19.

4 Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности: BS ISO/IEC 27005:2008. – Киев: 2011. – 70 с.

5 ГОСТ Р ИСО/МЭК 13335-1 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: – Введ. 2007.05.31. – М.: ИПК «Издательство стандартов», 2007. – ч.1. 23 с.

6 ГОСТ Р ИСО/МЭК 18045–2008. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий = Information technology. Security techniques. Methodology for IT security evaluation.: – Введ. 2008.12.18. – М.: ИПК «Издательство стандартов», 2008. – 234 с.

7 Петренко С.А., Симонов. С. В. Управление информационными рисками. Экономически оправданная безопасность – М.: Компания АйТи, ДМК Пресс, 2004. – 384 с.

8 Information technology, Security techniques, Code of practice for information security management: ISO/IEC 27002:2005 // International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2005. – 171 p.

9 Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013 // International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2013. – 34 p.

10 Симонов С. В. Анализ рисков в информационных системах. Практические аспекты. Защита информации // Конфидент. Безопасность компьютерных систем – 2001. – №2. – С. 48-53.

11 Симонов С. В. Технологии и инструментарий для управления рисками. // Информационный бюллетень JetInfo. – 2003. – № 2 (117) – С. 3 – 32.

12 Медведовский И. С. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ // SecurityLab. Электрон. дан. – // WorldWideWeb. – URL: http://www.ixbt.com/cm/informationsystem-risks012004.shtml. – Загл. с экрана (просмотрено 18 декабря 2014).

13 Ахметов Б.Б. Использование аппарата нечеткой логики для оценки риска информационной безопасности вуза // Поиск. Серия технических и естественных наук, 2009. – №3. – С.235-240.

14 Ахметов Б.С., Жекамбаева М.Н., Корченко А.Г., Казмирчук С.В. Методы оценивания рисков для систем управления информационной безопасностью // Вестник Национальной академии Республики Казахстан. – 2015. – №,6. – С. 23-38.

15 Ахметов Б.С., Надеев Д.Н., Фунтиков В.А., Иванов А.И., Малыгин А.Ю. Оценка рисков высоконадежной биометрии. – Алматы: КазНТУ, 2014. – 108 с.

16 Дзекцер Е.С. Геологическая опасность и риск (методологическое исследование) // Инженерная геология. – 1992. – № 6. – С. 3-10.

17 Atymtayeva L. Development of Expert Systems for Information Security Active Audit. // Proceedings of the 16th International Symposium on Advanced Intelligent Systems. Mokpo: Korea, 2015. F1C-4, p. 1-12.

18 Atymtayeva L., Abdel-Aty M. Improvement of Security Patterns strategy for Information Security Audit Applications //Proceeding softhe Fifth International Symposium on Business Modeling and Software Design, BMSD. Milan: Italy, 2015. p.199-205.

19 Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения – Киев. «МК-Пресс», 2006. – 320 с.

20 Mazin Al Hadidi, Jamil Samih Al-Azzeh, B. Akhmetov, O. Korchenko, S. Kazmirchuk, M. Zhekambayeva. Methods of Risk Assessment for Information Security Management// International Review on Computers and Software (I.RE.CO.S.)– 2016. –Vol. 11, №2. – 81-91 p.

21 Peltier T.R. Information security risk analysis – London: Auerbach Publications, 2001. – 281 p.

22 Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft: учебный курс. – Санкт-Петербург: Издательство «INTUIT», 2009. – 136 с.

23 Рагозин Ф. Оценка и картографирование опасности и риска от природных и техногенных процессов (теория и методология) // Проблемы безопасности при чрезвычайных ситуациях. – 1993. - №5. – 16–41 с.

24 Мушик Э., Мюллер П. Методы принятия технических решений. – М.: Мир, 1990. – 206 с.

25 Маршалл В.К. Основные опасности химических производств – М.: Мир, 1989. – 672 с.

26 Костров Д.Д. Анализ рисков и управление ими // Byte Россия. – 2003. – №10 (62) – 15–20 с.

27 Фишберн П. Теория полезности для принятия решений. – М: Наука, 1978. – 352 с.

28 Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений – 4-е изд., – М.: Азбуковник, 1999. – 944 с. – (Российская академия наук. Институт русского языка им. В. В. Виноградова).

29 Кондратьев М.Ю., Ильин. В.А. Азбука социального психолога-практика: Справочно-энциклопедическое издание – М: ПЕР СЭ, 2007. – 464 с.

30 Петровского А. В., Карпенко Л. А., Венгер А. Л. Социальная психология – М.: ПЕР СЭ, 2005. – 176 с.

31 Ребера А. Оксфордский толковый словарь по психологии – Oxford: Penguin Non-Classic, 2002. – 864 с.

32 Индеева В.В. К вопросу об определения понятия «риск» – М.: Российская Академия Естествознания, 2009. – Режим доступа: World Wide Web. – URL: http: http://www.rae.ru/zk/arj/2007/02/Indeeva.pdf. – Загл. с экрана (просмотрено 20 апреля 2010).

33 Широков К. П. Большой советской энциклопедии – М.: Печь – Польцин, 1955. – 669 с.

34 Википедия: Свободная энциклопедия. – Электрон. дан. – Сан-Франциско: Фонд Викимедиа, 2012. – Режим доступа: World Wide Web. – URL: http://ru.wikipedia.org/?oldid=44986537. – Загл. с титул. экрана. – Описание на основе версии, датированной 3 июня 2012 08:54 UTC.

35 Rowe W. An anatomy of risk. / W. Rowe – NY/: John Wiley, 1997. – 488 p.

36 U. S. Geological Survey: Proposed procedures for dedealing with warning and preparedness for geologic-related hazard // United States Federal Register. – 1977, 42. №70. – 14292–14296 p.

37 Fiksel J. Quantitative risk analysis for toxic chemicals in the environment // of hazard materials. – 1987. – 10, № 2-3. – 227–240 p.

38 Соловьев С.Ю., Казеннова Н.В., Гинкул Г.П. Глоссарий: Служба тематических толковых словарей. – Электрон. дан. – М.: ООО “Web and Press”, 2000–2010. – Режим доступа: World Wide Web. – URL: http://www.glossary.ru/. – Загл. с экрана (просмотрено 25 апреля 2010).

39 Коноплицкий В.А., Филина А.И. Толковый словарь экономических терминов. – Киев: Издательство «Альтерпресс», 1996. – 184 с.

40 Словарь по экономике и финансам. Глоссарий. ру // Яндекс: [интернет-портал]. – Электрон. дан. – М.: 2010. – Режим доступа: World Wide Web. – URL: http://slovari.yandex.ru/dict/glossary. – Загл. с экрана (просмотрено 19 декабря 2014).

41 Страховой бизнес: словарь-справочник – Электрон. дан. – М.: Международный Институт Исследования Риска, 2010. – Режим доступа: World Wide Web. – URL: http://www.miir.ru. – Загл. с экрана (просмотрено 20 мая 2015).

42 Термінологія в галузізахистуінформації в комп’ютерних системах віднесанкціонованого доступу [Текст]: НД ТЗІ 1.1-003 – 1999. – Чин. 1999. 04.28. – К. : ДСТСЗІ СБ України, 1999. – 12 с.

43 Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary

Stoneburner, Alice Goguen, Alexis Feringa]: National Institute of Standards and Technology Special Publication 800-30 – Falls Church: Natl. Inst. Stand. Technol, 2002. – 54 p.

44 ГОСТ Р ИСО/МЭК 15026 – 2002. Информационная технология. Уровни целостности систем и программных средств: Введ. 2003.06.30. – М.: ИПК "Издательство стандартов", 2003. – 15 с.

45 Control Objectives for IT and reated Technology Framework Control Objectives Management Guidelines Maturity Models: COBIT 4.1. – Rolling Meadows: IT Governance Institute, 2007. – 196 p.

46 ГОСТ Р 51897–2002. Менеджмент риска. Термины и определения: – Введ. 2001.05.31. – М.: ИПК «Издательство стандартов», 2002. – 8 с.

47 Руководство по управлению рисками безопасности. Центр Microsoft security centerof excellence // TechNet. – Электрон. дан. – Редмонд, США: Корпорация Майкрософт, 2006. – Режим доступа: WorldWideWeb. – URL: http://technet.microsoft.com/ru-ru/library/cc163143.aspx. – Загл. с экрана (просмотрено 29 декабря 2014).

48 ГОСТ Р 51901 – 2002. Управление надежностью. Анализ риска технологических систем: – Введ. 2003.09.01. – М.: ИПК «Издательство стандартов», 2002. – 21 с.

49 Risk management. Vocabulary: ISO Guide 73:2009 // International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). – 2002. – 15 p.

50 Лопатников Л. И. Экономико-математический словарь // Словарь современной экономической науки. – 5-е изд., перераб. и доп. – М.: Дело, 2003, – 520 с.

51 Российская энциклопедия по охране труда: [В 3 т.]. – 2-е изд., перераб. и доп. – М.: Изд-во НЦ ЭНАС, 2007. – Т. 2: Л – Р. – 408 с.

52 A Guide to risk assessment and safeguard selection for Information Technology Systems: MG-3 K1G 3Z4 – Ontario: Government of Canada, Communications Security Establishment (CSE) P.O., 1996. – 65 p.

53 Качинський А.Б. Аналіз ризику – методологічна основа для розв'язання проблем безпеки людини та довкілля: Серія «Екологічна безпека». Екологічна безпека України. Системний аналіз перспектив покращення. Розділ 3 / – Електрон. дан. – К.: Національний інститут стратегічних досліджень – 2001. – Режим доступу: WorldWideWeb. – URL: http://www.niss.gov.ua/book/Kachin/1-3.htm. – Загл. з екрану (переглянуто 15 березня 2015).

54 Smith M. Commonsense Computer Security, your practical guide to information security / M. Smith // London: McGraw – Hill, 1993 – 105 p.

55 Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA. [Electronic resource] / Security Risk Analysis & Assessment, and ISO 27000 Compliance –Electronic data – Macclesfield: The Leading Security Risk , 2010– Access mode: World Wide Web. – URL: http://www.riskworld.net/.

56 Alberts C. J., Behrens S. G., Pethia R. D., Wilson W. R. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM). – Hanscom: SEI Joint Program Office, 1999. – 72 p.

57 Taha, Hamdy A. Operations Research. An Introduction. – New York: MacMillan Publishing Company, 1987. – 123 p.

58 Жекамбаева М.Н. Ақпараттық қауіпсіздік қатерін бағалау амалдарының анализі //Вестник Восточно-Казахстанского государственного технического университета имени Д.Серикбаева. – 2015. – №4(70). – 95-101 с.

59 Жекамбаева М.Н., Казмирчук С.В. Программные средства оценивания рисков информационной безопасности //Доклады Национальной академии Республики Казахстан. – 2015. – №6. – 43-54 с.

60 Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA. [Electronic resource] / Security Risk Analysis & Assessment, and ISO 27000 Compliance –Electronic data – Macclesfield: The Leading Security Risk, 2010– Access mode: World Wide Web. – URL: http://www.riskworld.net/.

61 Корченко А.Г., Казмирчук С.В., Алимсеитова Ж.К., Жекамбаева М.Н. Программное средство оценивания рисков информационной безопасности COBRA //Сборник трудов III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан-2050». – Астана: Евразийский национальный университет имени Л.Н.Гумилева. – 2015. – 197-202 с.

62 Медведовский И. С. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ [Электронный ресурс] // SecurityLab. Электрон. дан. – Мн.: SecurityLab, 2004. – Режим доступа: World Wide Web. – URL: http://www.ixbt.com/cm/informationsystem-risks012004.shtml. – Загл. с экрана (просмотрено 18 декабря 2014).

63 Ахметов Б.С., Жекамбаева М.Н., Корченко А.Г., Казмирчук С.В. Программное средство оценивания рисков информационной безопасности CRAMM //Сборник трудов III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан-2050». – Астана: Евразийский национальный университет имени Л.Н. Гумилева. – 2015. – 202-207 с.

64 Рекомендации в области стандартизации банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности [Электронный ресурс]: РС БР ИББС-2.2-2009. – Введ. 2010.01.01 // Банк России: Официальный сайт. – Электрон. дан. – М.: Банк России. – Режим доступа: World Wide Web. – URL: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf. – Загл. с экрана (просмотрено 29 декабря 2014).

65 Risk management: Standard AS/NZS 4360:2004/ – Nundah: ISO working group – risk management Terminology, 2004. – 65 p.

66 Compliant Information Security Risk Assessment Tool: vsRisk [Electronic resource] / IT Governance Ltd. –Electronic data – Boise: IT Governance Ltd, 2011. – Access mode: World Wide Web. – URL: http://www.27001.com/products/31.

67 Callio Technologies: программный комплекс управления политикой информационной безопасности компании (международный стандарт BS7799 ISO 17799) [Электронный ресурс] // CallioTechnologies. – Электрон. дан. – М.: Представительство Callio Technologies, 2012. – Режим доступа: World Wide Web. – URL: http://businesssoft.ru.– Загл. с экрана (просмотрено 18 марта 2015).

68 Jeevan Jaisingh Value at Risk: A methodology for Information Security Risk Assessment / Jeevan Jaising, Jackie Rees Krannert // Proceedings of The 6th INFORMS Conference on Information Systems and Technology (CIST-2001). – Miami Beach, Florida, November 2001. –15 p.

69 Частиков А. П., Леднева И. Ю. Использование байесовской сети при разработке экспертных систем с нечеткими знаниями – Электрон. дан. – Краснодар: Кубанский государственный технологический университет, 2005. – Режим доступа: World Wide Web. – URL: http://ito.su/2000/II/5/5152.html.

70 Syalim A. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST 800-30 and Microsoft's Security Management Guide / A. Syalim, Y. Hori, K. Sakurai // International Conference on Issue – Fukuoka: Grad. Sch. of Inf. Sci. &Electr. Eng. – 726–731 p.

71 International standard Risk management. Principles and guidelines: ISO/FDIS 31000:2009(E) / International Organization for Standardization // JISC – 2009. – 24 p.

72 Risk analysis based on IT-Grundschutz: BSI-Standard 100-3 – Boon: Bundesamtfür Sicherheit in der Information stechnik, 2008. – 23 p.

73 Risk Management Tools. Program Risk Management Tools [Electronic resource] / The MITRE Corporation. All rights reserved – New York: Solutions That Make a Difference, 2012. – Access mode: World Wide Web. – URL: http://mitre.org/work/systems_engineering/guide/risk_management_tools.html.

74 MEHARI – Overview / Club de la Securit ´ e de l'Information Franc¸ais – Paris: CLUSIF, 2010 – 50 p.

75 MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. Book I –The Method / [version 2]. – Madrid: Ministerio de administra cionespúblicas, 2006. – 140 p.

76 CMS Information Security Risk Assessment (RA) Methodology / [CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)] – Baltimore: Centers for Medicare & Medicaid Services, 2002. – 21 p.

77 Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Кортежная модель базовых характеристик риска //Вестник Казахского национального технического университета имени К.И.Сатпаева. – 2015. – №6(112). – 268-288 с.

78 Ахметов Б.С., Корченко А.Г., Жекамбаева М.Н., Казмирчук С.В. Қауіптің базалық сипаттамасының кортежді моделі //Қазақстан

Республикасының ұлттық ғылым академиясының баяндамалары. – 2015. – №6. – 12-19 б.

79 Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Методы преобразования лингвистических переменных для системоценивания рисков //Актуальніпитаннязабезпеченнякібербезпекитазахистуінформації»: ТезидоповідейучасниківIIміжнародноінауково-практичноіконференції. – 2016. – 15-19 с.

80 Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Система оценивания рисков на базе метода FirstM //Сборник статей XV Международной научно-технической конференции «Проблемы информатикив образовании, управлении, экономике и технике». – Пенза: Приволжский дом знаний. – 2015. – 105-110 с.

81 Жекамбаева М.Н., Ахметова С.Т., Алимсеитова Ж.К. Система оценивания рисков на базе метода SecondM // Сборник статей XV Международной научно-технической конференции «Проблемы информатики в образовании, управлении, экономике и технике». – Пенза: Приволжский дом знаний. – 2015. – 111-116 с.

82 Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Метод n-кратного инкрементирования числа термов лингвистических переменных в задачах анализа и оценивания рисков // Научный журнал «Безпека інформації». – Киев, 2015. – Т.21. – №2. – 191-200 с.

83 Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Метод n-кратного инкрементирования порядка лингвистических переменных на основе частного расширения базы //Научный журнал «Защита информации». – Киев, 2015. – № 3(17). – 231-239 с.

84 Korchenko O., Kazmirchuk S., Akhmetov B., Zhekambaeva M. Increment Order of Linguistic Variables Method in Information Security Risk Assessment// Problems of Infocommunications. Science and Technology: 2015 Second International Scientific-Practical Conference, October 13-15, 2015: abstracts Kharkiv, 2015. 259-262 p.

85 Ахметов Б.С., Жекамбаева М.Н., Корченко А.Г., Казмирчук С.В. Синтез систем оценивания рисков информационной безопасности //Труды II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика». – Алматы: КазНИТУ имени К.И.Сатпаева. – 2015. – Т. II. – 35-39 с.

ҚОСЫМША А

ҚБАҚ АҚ жүйесінің бағдарламалық мәтінінің үзіндісі

```
#include <vcl.h>
#pragma hdrstop
#include "Unit1.h"
#include "Unit2.h"
//---------------------------------------------------------------------------
#pragma package(smart_init)
#pragma link "dxdbtree"
#pragma link "dxtree"
#pragma resource "*.dfm"
TForm1 *Form1;
//---------------------------------------------------------------------------
__fastcall TForm1::TForm1(TComponent* Owner)
        : TForm(Owner)
{
}
//---------------------------------------------------------------------------
void __fastcall TForm1::RadioGroup1Click(TObject *Sender)
{
if (RadioGroup1->ItemIndex == 0)
        {
        Edit1->Visible = true;
        ComboBox1->Visible = false;
        }
if (RadioGroup1->ItemIndex == 1)
        {
        Edit1->Visible = false;
        ComboBox1->Visible = true;
        }
}
//---------------------------------------------------------------------------
void __fastcall TForm1::Button1Click(TObject *Sender)
{
if (RadioGroup1->ItemIndex == 0)
        {
                if (Edit1->Text != "")
                        {
                        ADOQuery1->Close();
```

```
                        ADOQuery1–>SQL–>Clear();
                        AnsiString tn = "CREATE TABLE " + Edit1–>Text + "(id int
AUTO_INCREMENT PRIMARY KEY, resource varchar(200) NOT NULL, threat
varchar(200) NOT NULL, probability int(5) NOT NULL, frequency decimal(4,2)
NOT NULL, loss decimal(4,2) NOT NULL, danger int(5) NOT NULL, dr
decimal(4,2))";
                        ADOQuery1–>SQL–>Add(tn);
                        ADOQuery1–>ExecSQL();

                        ADOQuery2–>Close();
                        ADOQuery2–>SQL–>Clear();
                        tn = "CREATE TABLE " + Edit1–>Text + "(id int
AUTO_INCREMENT PRIMARY KEY, resource varchar(200) NOT NULL, risk
decimal(4,2) NOT NULL, lp varchar(100))";
                        ADOQuery2–>SQL–>Add(tn);
                        ADOQuery2–>ExecSQL();
                        Hide();
                        Application–>CreateForm(__classid(TForm2), &Form2);
                        Form2–>Label1–>Caption = Form2–>Label1–>Caption +
Edit1–>Text;
                        Form2–>Label2–>Caption = Edit1–>Text;
                        Form2–>ShowModal();
                        Close();
                        }
                    else
                        {
                        ShowMessage("Жоба атын енгізініз");
                        }
            }
        if (RadioGroup1–>ItemIndex == 1)
            {
                    if (ComboBox1–>ItemIndex != –1 )
                        {
                        Form2–>ADOQuery1–>Close();
                        Form2–>ADOQuery1–>SQL–>Clear();
                        AnsiString tn = "select * from " + ComboBox1–>Text;
                        Form2–>ADOQuery1–>SQL–>Add(tn);
                        Form2–>ADOQuery1–>Open();
                        Hide();
                        Application–>CreateForm(__classid(TForm2), &Form2);
                        Form2–>Label1–>Caption = Form2–>Label1–>Caption +
ComboBox1–>Text;
                        Form2–>Label2–>Caption = ComboBox1–>Text;
                        Form2–>ShowModal();
```

```
                    Close();
                    }
            }
        }
        //---------------------------------------------------------------------------
---
        void __fastcall TForm1::FormShow(TObject *Sender)
        {
        Form2->ADOres->GetTableNames(ComboBox1->Items, false);
        }
        //---------------------------------------------------------------------------
---
```