Әл-Фараби атындағы Қазақ ұлттық университеті

ӘОЖ 004.056 Қолжазба құқығында

АДИЛЖАНОВА САЛТАНАТ АЛЬМУХАНБЕТОВНА

Киберқауіпсіздік ресурстарын динамикалық басқару үшін ақпараттық технологиялар және әдістер мен модельдер

8D06301 – «Ақпараттық қауіпсіздік жүйелері»

Философия докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

Ғылыми кеңесшілер:
техника ғылымдарының докторы,
профессор Ахметов Б. С.,
техника ғылымдарының докторы,
профессор Лахно В. А. (Украина)

Қазақстан Республикасы
Алматы, 2023

МАЗМҰНЫ

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

АҚ – ақпаратты қорғау;
АҚ – ақпараттық қауіпсіздік;
АКЖ – ақпараттық-коммуникациялық жүйе;
АР – ақпараттық ресурс;
АЖ – ақпараттық жүйе;
АО – ақпараттандыру объектісі;
АҚҚ – ақпаратты қорғау құралдары
АЖТ – ақпараттық жүйелер мен технологиялар;
АҚБЖ – ақпараттық қауіпсіздікті басқару жүйесі.
БҚ – бағдарламалық қамтамасыз ету;
БП – бағдарламалық пакет;
ГА – генетикалық алгоритм;
КҚ – киберқауіпсіздік;
КФЖ – киберфизикалық жүйе;
МФ-мақсат функция
МГА – модификацияланған генетикалық алгоритм;
ШҚТ – шешім қабылдаушы тұлға;
ШҚҚЖ – шешім қабылдауды қолдау жүйесі;
DSS- decision support systems

КІРІСПЕ

Шешілетін ғылыми немесе ғылыми технологиялық проблеманың заманауи жай-күйін бағалау

Қорғау және шабуыл жасау тараптарының тұрақты қарсы тұруы жағдайында кез келген ақпараттандыру объектісінің ақпаратты қорғау (АҚ) қызметінің мақсаты шабуылдаушы тараптың әрекеттерінің салдары ретінде оны ұрлау, бұрмалау, құпиялылықты жоғалту мүмкіндіктерін барынша азайту болып табылады. Сондай-ақ, шабуылдаушылардың диаметрлі қарама-қарсы есептері − өз ресурстарын АОБ ақпараттық ресурстарына (АР) қол жеткізуге арналған шығындарды барынша азайтатындай етіп бөлу.

Қорғау тарабының шектеулі ресурстарын (материалдық, адами, қаржылық және т.б.) тиісті түрде бөлу кибернетикалық (КҚ) немесе ақпараттық қауіпсіздік (АҚ) саласындағы зерттеудің көптеген бағыттарының мәні болады. АҚ және КҚ-ға қатысты мұндай амал қорғаныс объектілері арасында ресурстарды бөлуді ұтымды шешу есебін қоюға әкеледі. Бұл тапсырманың бірнеше аспектілері болады және шешім техникасын таңдауды және түпкі нәтижені анықтайтын жағдай туралы белгілі бір білімді қажет етеді. Қорғау объектілерінің әрқайсысы туралы мұндай білімге мыналар жатады: ақпараттық ресурстардың (бұдан әрі − АР) саны, сапасы және маңыздылығы; АР қорғалуының бар деңгейі; оқиғаның күтілетін ықтималдығын ескере отырып, шабуыл жасау тарапы (немесе тараптар) бағыттай алатын ресурстардың (материалдық, қаржылық, адами, т. б.) саны; ақпараттандыру объектісін (АОБ) қорғау тарабы бөлуі мүмкін ресурстардың саны; АР жоғалту тәуекелінің жол берілетін деңгейі.

Ақпараттық саладағы қарсылық есептеріндегі зерттеулерді талдау ақпарат ағындарының үнемі өсуіне және олардың маңыздылығына байланысты шабуылдардың қарқындылығы артатынын көрсетеді. Мұнда шабуылдар санының өсу трендісінің динамикасы қатарынан бірнеше ондаған жылдар бойы үздіксіз тіркеліп келеді. Яғни, бұл − үздіксіз процесс. Бұл қорғаныс тарапынан тиісті шаралар қабылдау қажеттілігін тудырады. Алайда шабуылдардың бағыттылығы уақыт өте келе өзгеруі мүмкін, ол шабуылдаушылардың объектілер арасындағы шабуыл векторына байланысты қорғаныс ресурстарын қайта бөлудің жаңа есептерімен бірге жүруі мүмкін. Қазіргі заманғы ақпараттық-коммуникациялық жүйелердің (АКЖ) көп деңгейлі құрылымы КҚ немесе АҚ кешенді жүйелерінің көп деңгейлі контурларын құруды анықтайды.

Тақырыпты әзірлеу үшін негіз және бастапқы деректер

Белгісіздік қарсыластың іс-әрекетін тек белгілі бір ықтималдықпен болжауға болатын кезде, теориялық- ойын әдістерін қолдану және қарама-қайшылық жағдайларының өзгеру динамикасын ескере отырып, АҚ объектілері арасында шектеулі ресурстарды ұтымды бөлуді іздеу ақпараттың қауіптерін жүзеге асырудан келтірілген зиянның мөлшерін ең аз шамаға дейін азайтуға мүмкіндік береді. Диссертациялық жұмыс тақырыбын әзірлеудің негізі − АКЖ-ның көп контурлы АҚҚ-ға арналған АҚҚ-ны таңдау кезінде көп критерийлі ұтымды шешу есебі арқылы АОБ-нің қауіпсіздік деңгейін жоғарылату мүмкіндігі туралы гипотеза. Бұл ретте АҚ және КҚ АОБ үшін көп контурлы

жүйелердің ұтымды конфигурацияларын іздеу барысында көптеген шешімдерді генерациялау үшін эволюциялық әдістер мен генетикалық алгоритмдерді дамытуға, сондай-ақ бар қауіптердің өзектілігіне сүйене отырып, қорғау тарабының ресурстарын динамикалық қайта бөлу жөніндегі есепті шешу үшін ГА-ны қолдануға назар аударған дұрыс.

Ғылыми-зерттеу жұмыстарын жүргізу қажеттілігінің негізі

Ресурстарды басқаруды модельдеу саласындағы ғылыми жұмыстарды талдау ақпаратты қорғау тараптары негізгі күш-жігердің қорғауға салынған инвестициялар көлемін анықтауға бағытталғанын көрсетеді. Бұл инвестицияларды қорғау объектілері арасында бөлу есеплері жекелеген зерттеулерге арналған. Сонымен қатар, қолданыстағы әзірлемелер шабуылдаушының ықтимал әрекеттері мен олардың салдарының АОБ-дағы АЖ көрсеткіштері мен сипаттамаларының өзгеруіне әсерін сирек ескереді. Шабуылдар санының өсуі жағдайында шаруашылық қызмет субъектілерінің ақпаратын қорғауға бөлінетін шектеулі қаржы ресурстарын тиімді пайдалану есебі барған сайын маңызды бола түсуде және кез келген мемлекеттің АҚ және КҚ деңгейін айтарлықтай дәрежеде айқындайды. Сонымен қатар, белгісіздікте шабуылдаушы тараптың әрекеттерінің дәйектілігі алдын-ала белгісіз және белгілі бір ықтималдықпен мақсатты шабуыл сценарийін болжауға болған кезде, теориялық және ойын әдістерін қолдану және қарама-қайшылық жағдайларының өзгеру динамикасын ескере отырып, АҚ объектілері арасында шектеулі ресурстарды ұтымды бөлуді іздеу ақпараттық ресурстардың ағып кетуінен қаржылық шығындарды ең аз шамаға дейін азайтуға мүмкіндік береді.

АҚҚ құнының өсуі қорғау ресурстарын ұтымды пайдалану проблемасын өзектендіреді. Шешімдерді іздеу барысында уақыт өте келе шабуылдаушы тараппен қарсыласу жағдайларының өзгеруін ескеру қажет. Бұл ақпараттық ресурстардың «ескіруіне», олардың жаңаруына, жаңа шабуыл құралдарының пайда болуына, АҚҚ модернизациясына және т.б. байланысты. Нәтижесінде біз күрделі қорғаныс құрылымдарындағы ресурстарды динамикалық басқару есебін шешу қажеттілігіне келеміз.

АОБ ақпараттық инфрақұрылымын талдау, АҚ және КҚ бағалау мен басқарудың кез келген әдістемесінің есепті кезеңі. Бұл талдау неғұрлым терең болса, бағалау нәтижесі соғұрлым объективті болады.

Осылайша, тиімді АҚҚ құру үшін кешенді түрде оның тиімділігін анықтайтын көрсеткіштердің жеткілікті үлкен санын ескеру қажет. Сонымен бірге, олардың талаптарының сәйкес келмеуіне байланысты әртүрлі көрсеткіштердің ұтымды мәндеріне қол жеткізу өте қиын және көбіне мүмкін емес. Нәтижесінде біз көп критерийлі есепке келеміз. Мұндай есепті шешу әрқашан да жеке көрсеткіштерге қойылатын талаптарды орындаудағы келісімге келу болып табылады. Мұндай көп критерийлі есептерді шешкен кезде әрдайым шешім алгоритмдерін таңдау дилеммасы пайда болады. Бұл, әсіресе, ақпаратты қорғауға байланысты есептерді қатысты, өйткені қорғау тарапының әрекеттері көбінесе белгісіздік жағдайында орындалады. Тиісінше, есептің тұжырымы және нәтижелері дәл болуы мүмкін емес. Егер нақты тәсілмен объективті функцияның экстремалды мәні оның сарапануына қатысты кейбір шарттарды орындау кезінде

бар болса және оны табуға болатын болса, онда нақты емес тәсілмен жеткіліксіз хабардарлық шешімнің қабылданбауына әкелуі мүмкін, ал АОБ-ны қорғаудың мақсаты берілген шектеулермен жеткілікті түрде қамтамасыз етілмеуі мүмкін.

Зерттеу тақырыбының өзектілігі. Қазақстан Республикасында ақпараттық саланың дамуы және оның көлемі мен құнының тиісті өсуі ҚР қоғамдық өмірінің барлық салаларына алдыңғы қатарлы ақпараттық технологиялардың енгізілуімен қатар жүреді, бұл шабуылдардың жиілігін және ақпараттың жайылып кетуінен болатын ықтимал залалды ұлғайтуға алып келеді. Нәтижесінде АҚҚ-ның күрделенеді және олардың құныны өседі. Мұндай жағдайларда шаруашылық қызмет субъектілерінің ақпаратын қорғауға шектеулі қаржы ресурстарын тиімді бөлу есебі барған сайын маңызды бола түсуде және айтарлықтай дәрежеде мемлекеттің ақпараттық (кибернетикалық) қауіпсіздігінің деңгейін айқындайды. Шабуыл жасаушылармен динамикалық қарама-қайшылық жағдайында АҚҚ көрсеткіштерін ұтымды шешу есептерін әзірлеу ерекше өзектілікке ие. Мұндай көрсеткіштер қорғаныс жүйесінің тиімділігін, ақпаратты қорғауға инвестиция салудан түсетін пайданы, олардың рентабельділігін және т.б. анықтайтын жоғалған ақпараттың үлесі болуы мүмкін. АОБ КҚ-ті қамтамасыз етумен байланысты есептерді шешу жолдарының жеткіліксіз теориялық және әдістемелік дамуы тақырыпты, мақсатты бағытты, зерттеудің мақсаттары мен есептерін таңдауға әкелді.

Диссертациялық жұмыстың мақсаты. Қаскүнемдердің іс-әрекеттерін ескере отырып, қорғау объектілері арасында ақпаратты қорғау ресурстарын ұтымды бөлу есебінен АОБ қорғалу деңгейін арттыру.

Осы мақсатқа жету үшін келесі есептерді шешу қажет:

1. АОБ АКЖ қауіпсіздігін басқару модельдерін, атап айтқанда, ақпаратты қорғау объектілері арасында қаражатты ұтымды бөлуді табуға арналған модельдерді талдау;
2. АОБ КҚ қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді ұтымды шешудің көп критерийлі есептерін шешу үшін МГА әзірлеу;
3. АКЖ қауіпсіздік контурлары үшін АҚҚ конфигурацияларының нұсқаларын іріктеумен және ұтымды шешумен байланысты есепті шешу үшін ГА-ны толықтыру;
4. Ақпаратты қорғау тарапының ресурстарды бөлуінің ұтымды нұсқасын талдау және таңдау үшін көп модульді ШҚҚЖ бағдарламалық түрде іске асыру.

Диссертациялық жұмыстың ғылыми жаңалығы:

1. Қауіптерді іске асырудан келтірілген залалды және ақпараттандыру объектісінің ақпараттық ресурстарының осалдығын сипаттайтын модельдің мақсатты функциясын таңдау әдістемесі **толықтырылды**, оның қолданыстағы шешімдерден айырмашылығы, кедергілерді еңсеру үшін айтарлықтай ресурстарды жұмсау қажет болатын компьютерлік жүйелерде айналатын ақпараттың қасиеттерін көрсететін бөлшек-сызықтық емес функцияларды таңдауды негіздейді.

2. МГА **алғаш рет** әзірленді, және қолданыстағы жобалардан айырмашылығы, ақпараттандыру объектілерінің киберқауіпсіздігін қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғаныс тарапының ресурстарын бөлудің көп критерийлік есепті ұтымды шешуді жеңілдетуге мүмкіндік береді. Бұл шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда - ақпараттандыру объектілерінің құрамындағы компоненттердің осалдығын төмендетуге бағытталған іс-шаралармен байланысты жұмыстарға ресурстарды бөлуді ұтымды шешуге және қол жеткізуді қамтамасыз ететін ресурстар көлемінің әртүрлі нұсқаларын модельдеуге мүмкіндік береді.

3. Ақпараттық - коммуникациялық жүйелердің қауіпсіздік контурлары үшін ақпаратты қорғау жүйесінің конфигурацияларының нұсқаларын таңдау және ұтымды шешумен байланысты есепті шешу үшін генетикалық алгоритм **одан әрі дамыды**. Қолданыстағы шешімдерден айырмашылығы- ақпаратты қорғау жүйесінің құрамын ұтымды шешу критерийі ретінде ақпараттың жоғалуынан болатын тәуекелдердің жиынтық шамасын, ақпаратты қорғау жүйесінің интегралды көрсеткіштерін, сондай-ақ ақпаратты қорғау жүйесінің әрбір классы үшін құн көрсеткіштерін пайдаланады.

Зерттеу есептері:

1. Ақпараттандыру объектісінің ақпараттық-коммуникациялық жүйелерінің қауіпсіздігін басқару модельдерін, атап айтқанда, ақпаратты қорғау объектілері арасында қаражатты ұтымды бөлуді іздеуге арналған модельдерді талдау

2. Ақпараттандыру объектісінің киберқауіпсіздігін қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді ұтымды шешудің көп өлшемді есептерін шешу үшін модификацияланған генетикалық алгоритм құру.

3. Ақпараттық-коммуникациялық жүйелердің қауіпсіздік контурлары үшін ақпаратты қорғау құралдарын конфигурациялау нұсқаларын іріктеумен және ұтымды шешумен байланысты есепті шешудің генетикалық алгоритмін толықтыру

4. Ақпаратты қорғау тарапының ресурстарды бөлудің ұтымды нұсқасын талдау және таңдау үшін шешімдер қабылдауды қолдаудың көп модульді жүйелерін бағдарламалық түрде іске асыру.

Зерттеу объектісі – объектілердің әлсіздігін ескере отырып, көп контурлы қорғаныс жүйелеріндегі ақпаратты қорғау ресурстарын динамикалық басқару процесі.

Зерттеу пәні – ақпаратты қорғау жүйесін құру кезінде қорғаныс тарабының ресурстарын басқару әдістері мен модельдері.

Диссертацияны метрологиялық қамтамасыз ету туралы мәліметтер

Диссертацияда келесі метрологиялық қамтамасыз ету қолданылды. Ақпаратты қорғау және ақпараттық қауіпсіздік жағдайында техникалық есептерді шешу үшін жалпы ғылыми және арнайы зерттеу әдістері қолданылды. Қорғаныс жағының ұтымды ресурстарын табу үшін Белман-Заде динамикалық бағдарламалау әдісі қолданылды. Жұмысқа АОБ КҚ қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлудің көп критерийлі ұтымды шешу есептері үшін эволюциялық (генетикалық) алгоритмдер кеңінен қосылған. АОБ КҚ күйлерін анықтау үшін дискретті және үздіксіз Марков тізбектері теориясының әдістері де қолданылды. Математикалық модельдеу үшін MathLab математикалық пакеттері қолданылды. Жұмыста ұсынылған ШҚҚЖ негізінде жүзеге асырылады. Графикалық әдістер диссертация материалдарын көрнекі түрде көрсету үшін қолданылды. Диссертацияда келтірілген теориялық есептеулердің деректері нәтижелерді енгізу туралы тиісті актілермен расталды.

Авторлық құқық куәлігі диссертацияның қосымшасында келтірілген

Диссертациялық жұмыстың практикалық құндылығы. «DSS dynamic allocation of cybersecurity resources» модульдік ШҚҚЖ әзірленді. Бұл бағдарламалық жасақтама MDI стилінде жасалған. «DSS Dynamic allocation of cybersecurity resources» ШҚҚЖ Visual Studio 2019 бағдарламалау ортасы, C# бағдарламалау тілінде жазылған және келісідей модульдер бағдарламалық түрде іске асырылған: 1-модуль – АҚҚ үшін АҚҚ жинақтарын және қорғау әдістерін қалыптастыру; 2-модуль – АҚҚ қорғау ресурстарын бөлуді ұтымды шешуге арналған модификацияланған генетикалық алгоритм (диссертацияның 2-ші және 3-ші тарауларында ұсынылған модельдер негізінде); 3-модуль – тораптар бойынша АҚҚ орналастыруды және АОБ қорғау жөніндегі шараларды ұтымды шешу (диссертацияның 2- тарауында ұсынылған модельдер негізінде); 4-Модуль – АОБ қорғау ресурстарын қайта бөлу икемделу функциясының өзгеру кестесі. «DSS Dynamic allocation of cybersecurity resources» ШҚҚЖ қолдану аппараттық және бағдарламалық жасақтаманың әртүрлі нұсқаларын және олардың АКЖ-ға арналған комбинацияларын жылдам сұрыптап қана қоймай, сонымен бірге диссертацияда берілген модельдер мен алгоритмдерді АОБ-ға АКЖ киберқауіпсіздік контурларының құрамын ұтымды шешу үшін қол жетімді модельдермен және алгоритмдермен біріктіруге мүмкіндік беретіні көрсетілген. Модельдер мен алгоритмдердің мұндай бірігуі АКЖ қорғанысын тез қалпына келтіруге мүмкіндік беретіні ықтимал. «DSS Dynamic allocation of cybersecurity resources» ШҚҚЖ практикалық құндылығы енгізу актілерімен расталған, атап айтқанда ШҚҚЖ функционалының кеңеюіне қарай оның архитектурасына ШҚҚЖ-ға есептеу өзегі үшін динамикалық қосылатын кітапханаларды қосу мүмкіндігімен ШҚҚЖ ашық көп модульді архитектурасының тиімділігі дәлелденген.

Қорғауға ұсынылатын тұжырым.

АКЖ қауіпсіздік контурлары үшін АҚҚ конфигурациясының нұсқаларын таңдау және ұтымды шешумен байланысты есепті шешу үшін ГА қолданылды және КҚ қамтамасыз ету бойынша жобаларды іске асыру процесінде қорғаныс тараптарының ресурстарын бөлуді ұтымды шешудің көп критерийлі есебін шешу үшін МГА қолданылды. Ақпаратты жоғалту тәуекелдерінің жалпы шамасын, АҚҚ интегралды көрсеткіштерін, сондай-ақ АҚҚ-ның әрбір классы үшін құндық көрсеткіштерді ескере отырып, ГА-ның ұсынылған модификациясы негізінде АҚҚ есептеу ядросына арналған динамикалық түрде қосылатын кітапхана түрінде модульді бағдарламалық жасақтама іске асырылды.

Диссертациялық жұмыс нәтижелерінің апробациясы.

Диссертацияның негізгі ережелері мен зерттеу нәтижелері Украинаның Ұлттық биоресурстар және табиғатты пайдалану университетінің компьютерлік жүйелер, желілер және киберқауіпсіздік кафедраларының ғылыми семинарында баяндалды және әл-Фараби атындағы ҚазҰУ ақпараттық технологиялар факультетінің және ақпараттық жүйелер кафедрасының ғылыми семинарларында, сонымен қатар мына төмендегі ғылыми-әдістемелік конференцияларда баяндалып талқыланды:

1. The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources // ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020,
2. Киберқауіпсіздік ресурстарын динамикалық басқарудың математикалық әдістерін талдау. // « Международная научная конференция студентов и молодых ученых «ФАРАБИ ӘЛЕМІ», КазНУ имени аль-Фараби, 2020
3. Анализ моделей информационной безопасности для задач распределения ресурсов стороны защиты // XX Международная научно-техническая конференция «Проблемы информатики в образовании, управлении, экономике и технике. – Пенза, 2020.
4. Использование генетического алгоритма в задаче динамического управления ресурсами кибербезопасности. // « Международная научная конференция студентов и молодых ученых «ФАРАБИ ӘЛЕМІ», КазНУ имени аль-Фараби, 2021.

Диссертациялық жұмысты орындаудағы алынған нәтижелер мен талдаулар бойынша 13 мақала жарық көрді және 1 авторлық куәлік алынды. Олардың ішінде Қазақстан Республикасы Білім және ғылым министрлігінің Білім және ғылым сапасын қамтамасыз ету комитеті ұсынған басылымдарда 5 (бес), «Scopus» базасына енгізілген 5 (бес), халықаралық конференциялар материалдарында 3 (үш) мақала жарық көрді.

Ғылыми жұмыстың жариялымдары.

1. Akhmetov, B., Lakhno V., Adilzhanova S. Automation of Information Security Risk Assessment. International Journal of Electronics and Telecommunications 2022, 68(3), pp. 549–555

2. Lakhno, V., Akhmetov, B., Adilzhanova, S., The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources // ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, стр. 251–254, 9349310

3. Lakhno V., Adilzhanova S., Kryvoruchko O., Desiatko A., Buriachok V., Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm. In: Silhavy R. (eds) Informatics and Cybernetics in Intelligent Systems. CSOC 2021. Lecture Notes in Networks and Systems, vol 228. Springer, Cham.

4. Akhmetov, B.,Lakhno, V., Adilzhanova, S., Conceptual Diagram of An Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems // Journal of Theoretical and Applied Information Technology, 2021, 99(18), стр. 4297–4310 .

5. Lakhno, V., Bereke, M., Adilzhanova, S., ...Desiatko, A., Palaguta, K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization // Journal of Theoretical and Applied Information Technology, 2022, 100(7), стр. 1693–1705.

6. Адилжанова С. А. Ақпараттандыру объектілерінің киберқауіпсіздік ресурстарының динамикалық басқарудың математикалық әдістерін талдау //Вестник КазНИТУ им.Сатпаева №3 (139). – 2020. –С. 102-106

7. Лахно В.А., Адилжанова С.А. Генетикалық алгоритмді кибер қауіпсіздік ресурстарының динамикалық бақылау есептерінде қолдану// Вестник КазНИТУ им.Сатпаева №6 (142). – 2020. – С. 565-568

8. Адилжанова С.А., Тюлепбердинова Г.А., Ақпараттандыру объектілерінің киберқауіпсіздік ресурстарын көп өлшемді ұтымды шешу мен динамикалық басқарудың математикалық әдістерін талдау // Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы, №4(72), 2020 с. 145-148

9. Ахметов Б.С., Адилжанова С.А., Қорғаныс объектілері арасында ресурстарды бөлуді ұтымды шешу кезінде шешім қабылдауды қолдаудың модульдік жүйесі // Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы №4(76), 2021 г.

10. Адилжанова С.А., Ахметов Б.С., Лахно В.А., Ақпаратты қорғау тарапының ресурстарын іріктеу, ұтымды шешу және қайта бөлу есепсін шешу үшін генетикалық алгоритмді дамыту. // Вестник Алматинского университета энергетики и связи No 1 (56) 2022

11. Адилжанова С.А. Киберқауіпсіздік ресурстарын динамикалық басқарудың математикалық әдістерін талдау. // « Международная научная конференция студентов и молодых ученых «ФАРАБИ ӘЛЕМІ», КазНУ имени аль-Фараби, 2020. – С.41

12. Адилжанова С.А Использование генетического алгоритма в задаче динамического управления ресурсами кибербезопасности. // « Международная научная конференция студентов и молодых ученых «ФАРАБИ ӘЛЕМІ», КазНУ имени аль-Фараби, 2021. – С.73

Диссертацияның құрылымы мен көлемі.

Диссертациялық жұмыс қазақ тілінде жазылды. Жұмыс төрт бөлімнен , қорытынды және қосымшалардан, әдебиеттер тізімінен тұрады. Диссертациялық жұмыстың жалпы көлемі 128 бет, 23 суреттен, 9 кестеден, 93 пайдаланылған дереккөзден және 2 қосымшадан тұрады.

1 КИБЕРҚАУІПСІЗДІК РЕСУРСТАРЫН ДИНАМИКАЛЫҚ БАСҚАРУ БОЙЫНША ЗЕРТТЕУ ЕСЕПТЕРІН ҚОЮ ЖӘНЕ ТАЛДАУ

1.1. Қорғау тарабының ресурстарын бөлу есептері үшін ақпараттық қауіпсіздік модельдерін талдау

Шектеулі ресурстарды тиісінше бөлу көптеген экономикасы дамып келе жатқан мемлекеттердің болмысын және сонымен бірге операцияларды зерттеу бағыттарының бірі – ұйымдық жүйелерді ұтымды басқару әдістерін әзірлеумен айналысатын ғылым саласын құрайды [1]. Ақпараттық және кибернетикалық қауіпсіздікке (бұдан әрі – тиісінше АҚ және КҚ) қатысты мұндай тәсіл қорғау объектілері арасында ресурстарды бөлуді ұтымды шешу есебін қоюға әкеледі. Мұндай объектілерге компьютерлік жүйелердің архитектурасына қарай (жергілікті, бөлінген) мыналар жатқызылуы мүмкін: үй-жайлар; ақпарат тасымалдағыштар; байланыс желілері және т.б.

Бұл тапсырманың бірнеше аспектілері бар және шешім әдістемесін таңдауды және түпкілікті нәтижені анықтайтын жағдай туралы белгілі бір білімді қажет етеді. Қорғау объектілерінің әрқайсысы туралы мұндай білімге мыналар жатады: ақпараттық ресурстардың (бұдан әрі – АР) саны, сапасы және маңыздылығы; АР қорғалуының бар деңгейі; оқиғаның күтілетін ықтималдығын ескере отырып, шабуыл жасау тарабы (немесе тараптар) бағыттай алатын ресурстардың (материалдық, қаржылық, адами, т.б.) саны; ақпараттық ресурстардың жеткілікті болуы үшін қажетті ресурстардың саны; ақпараттандыру объектісін (АОБ) қорғау тарабы бөлуі мүмкін ресурстар саны; АР жоғалту тәуекелінің жол берілетін деңгейі [2, 3].

Қорғаныс және шабуыл тараптарының тұрақты қарсылығы жағдайында ақпаратты қорғау (АҚ) қызметінің мақсаты шабуылдаушы тараптың әрекеттерінің салдары ретінде оны ұрлау, бұрмалау, құпиялылықты жоғалту мүмкіндіктерін азайту болып табылады. Сонымен қатар, шабуылдаушылар диаметрлі қарсы есептерге ие: өзінің ресурстарын АР АОБ-ке қол жеткізу шығындарын азайту үшін тарату.

Ақпараттық саладағы қарсыласу көрсеткіштерінің статистикасы [4-6], 1.1-1.5 суретті қараңыз, ақпарат ағынының үнемі өсуіне және олардың маңыздылығына байланысты шабуылдардың қарқындылығы артатынын көрсетеді. Сонымен қатар, шабуылдар санының өсу тенденциясы бірнеше ондаған жылдар бойы үздіксіз тіркеліп келеді. Яғни, бұл үздіксіз процесс. Бұл АҚ тарапынан тиісті шаралар қабылдау қажеттілігін тудырады. Алайда көзделген шабуылдар уақыт өте келе өзгеруі мүмкін, шабуылдаушылардың объектілер арасындағы шабуыл векторына байланысты қорғаныс ресурстарын қайта бөлудің жаңа есептерімен бірге жүруі мүмкін. Мұндай жағдай, мысалы, барлау жүргізу кезінде, шабуылдаушы тараптың объектілер бойынша ақпаратты бөлу туралы ақпараты болмаған кезде туындайды. Сондықтан егер барлау кезеңі шабуылдаушылар үшін сәтті жүргізілсе, онда олар өз күштерін өздері үшін тиімді бағытқа бағыттауға мүмкіндік алады. Шабуыл ресурстарын қайта бөлу қорғаныс тарапының жауапты реакциясын тудырады, ол өз ресурстарын шабуылдаушылардың тактикасына сәйкес қайта бөледі.

Ақпараттық-коммуникациялық жүйелердің (АКЖ) және киберфизикалық жүйелердің (КФЖ) қабілеттілігіне кепілдік беру қабілеті шеңберінде [7] олардың функционалдық және АҚ (КҚ) қамтамасыз етуге бағытталған іс-шаралар қажет. АКЖ және КФЖ (бұдан әрі – АКЖ) көп деңгейлі құрылымы КҚ немесе АҚ кешенді жүйелерінің көп деңгейлі контурларын құруды негіздейді. Іс жүзінде кибернетикалық, коммуникациялық және физикалық платформалардың АҚ-сын қамтамасыз ету қажет. АКЖ үшін ақпаратты қорғаудың кешенді жүйелерінің (АҚКЖ) негізі «объект – қауіп – қорғау» тұжырымдамасы болып табылады [8]. Осы тұжырымдама КҚ қамтамасыз етуге бағытталған: кибернетикалық платформа – ақпараттық ресурстар (АР), ақпараттық жүйелер (АЖ), коммуникациялық платформаның ақпараттық процестері (АП) – физикалық платформаның ақпараттық желілері және арналары (АЖ(А)) – датчиктер (Д).

Ресурстарды әзірлеу, енгізу, қызмет етуі, мониторингілеу, талдау, қолдау, жетілдіру және қарқынды басқару контексінде қорғау тараптары АКЖ үшін АҚ тәуекелдерін ескеретін жалпы басқару жүйесінің бөлігі ретінде АҚ (КҚ) басқару жүйесі (бұдан әрі – АҚҚ) өзекті болып табылады. АҚ басқарудың стандартталған модельдері белгілі [9, 10]. Шешілетін есептің мәтінінде «жоспарла - орында - тексер - әрекет ет» моделі кеңістігіндегі АКЖ АҚ басқару әдістемесін әзірлеудің келешегі зор болып табылатынын ескертеміз [11].

АОБ АҚ басқару тұжырымдамалары: АҚ қағидаттары, активтер, қауіптер, әлсіздіктер, әсер ету, тәуекел, қорғау шаралары мен шектеулер негізінде қалыптастырылды [12]. АҚКЖ-ның тиімді жұмыс істеуі үшін АҚ-ның мынадай жоғары деңгейлі қағидаттары іргелі болып табылады:

тәуекел менеджменті – активтер тиісті шаралар қабылдау арқылы қорғалуы керек. Қорғау шараларын таңдау және қолдану тәуекелдерді басқарудың тиісті әдіснамасы негізінде жүзеге асырылады. Әдістеме АОБ активтеріне, қауіптерге, әлсіздіктерге және қауіп-қатердің әртүрлі сипатына байланысты таңдалады. Әдістеме рұқсат етілген тәуекелдерді белгілейді және бар шектеулерді ескереді;

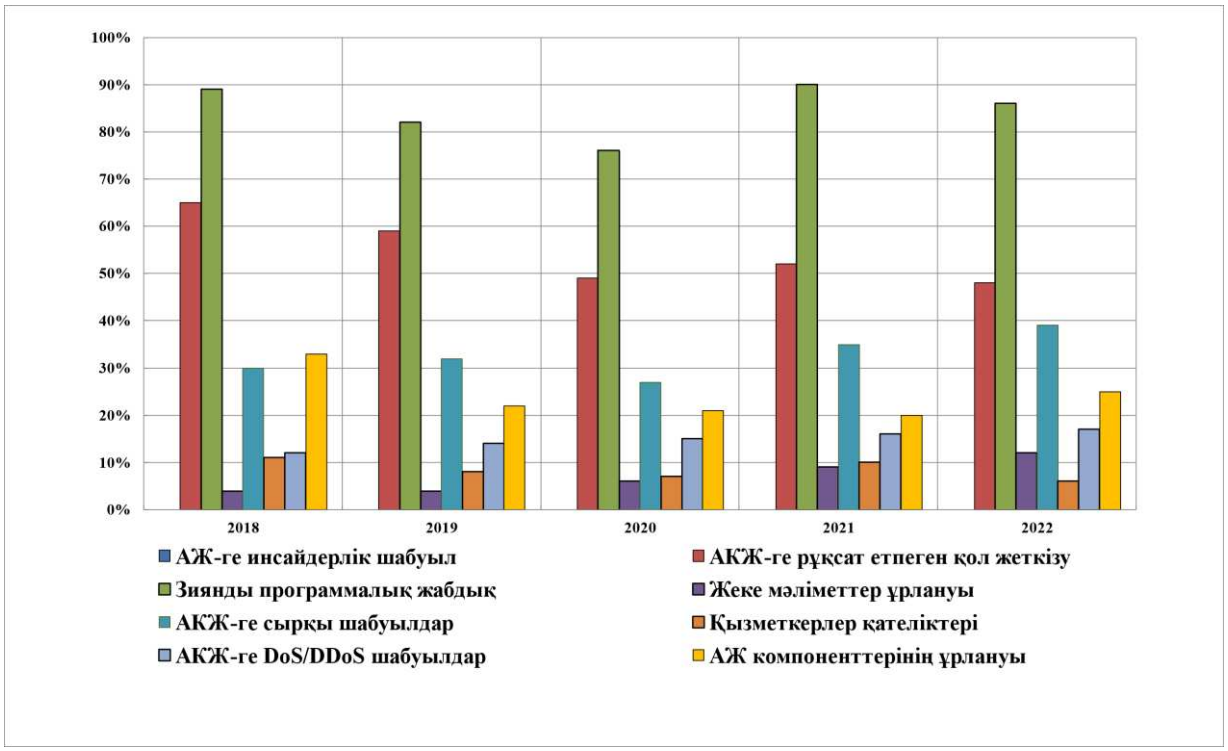
есептемелер – АКЖ АҚ саласында және тәуекелдерді басқаруда маңызды рөл атқарады. Есептемелерді қалыптастыру үшін АҚ-ның (АҚП) нақты саясаттарын іске асырудың әлсіз және күшті жақтарын анықтау қажет;

қызметтік есептер және жауапкершілік. АОБ басшысы мен менеджменті АҚ активтерін (АР) қамтамасыз етуге жауапты; қызметтік есептер мен жауапкершілік АКЖ АҚ-мен байланысты және айқындалуы, персоналдың назарына жеткізілуі тиіс [12, 125-126 б.];

АКЖ АҚ-мен байланысты тәуекелдерді басқару процесінде мақсаттарды, стратегияларды және АҚП-ны назарға алған жөн;

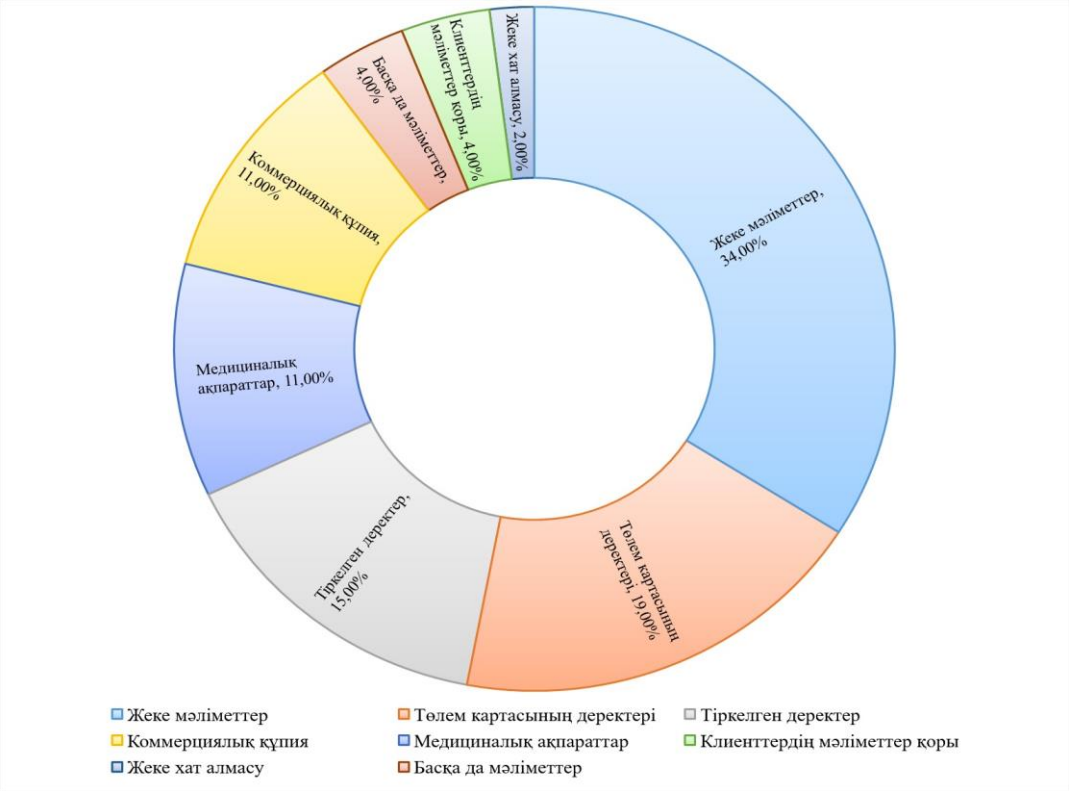
өмірлік циклды басқару – АКЖ АҚ басқару тұрақты болуы керек (АКЖ өмірлік циклі бойында).

АКЖ АҚ-ны қамтамасыз ету есебі – әртүрлі тұрғыдан қарастыруға болатын қорғаныс процестерін ұйымдастырудың көпжоспарлы есебі. АҚ элементтерінің өзара байланысы 1.6. суретте көрсетілген.

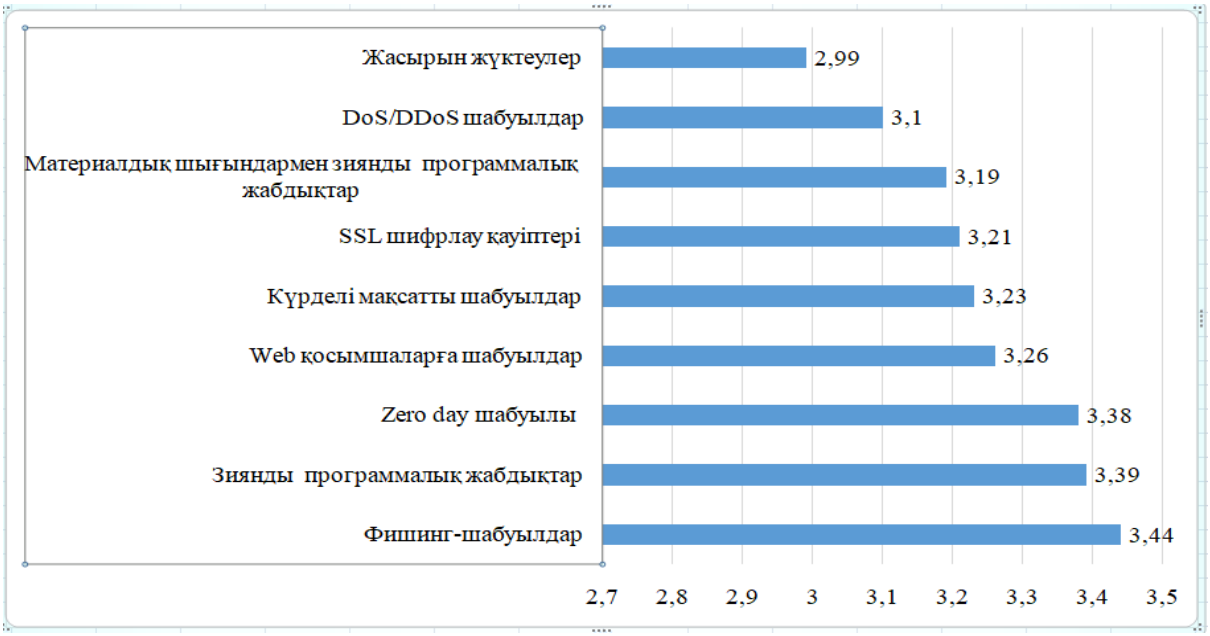


Сурет 1.1. 2018-2022 жылдар аралығында кибершабуыл статистикасы

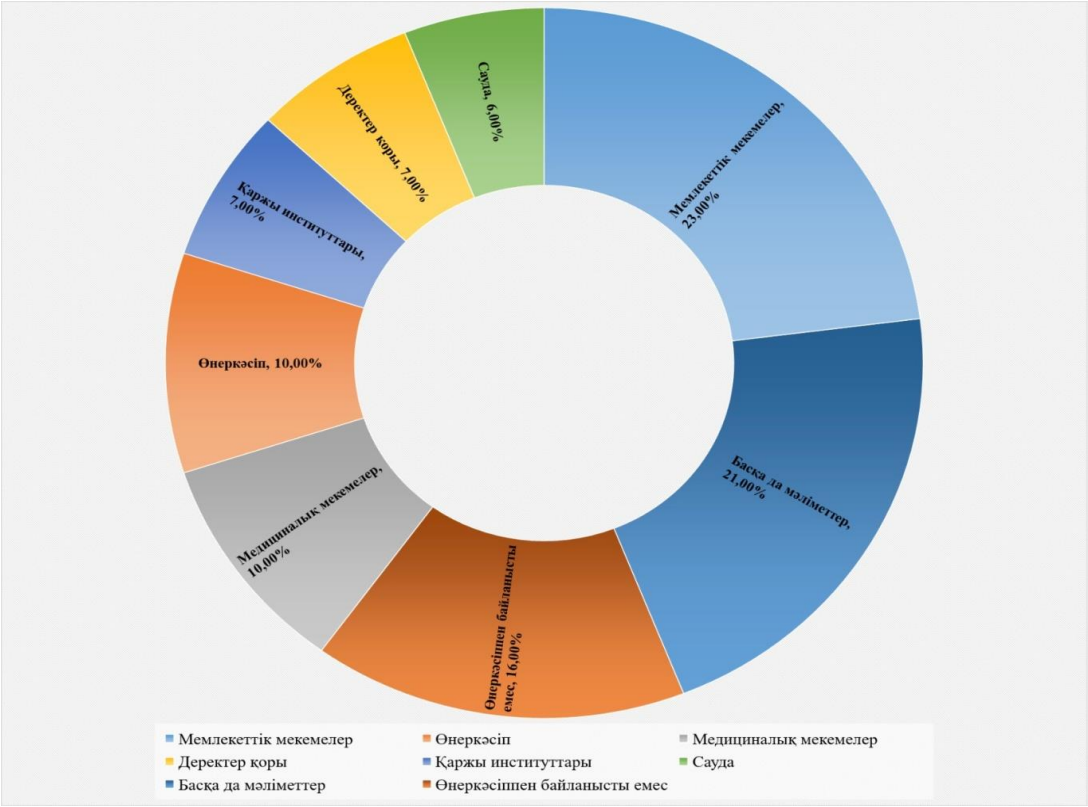
1.2-сурет. Жеке тұлғаларға жасалған кибершабуылдар нәтижесінде ұрланған деректердің түрлері (2018-2022)



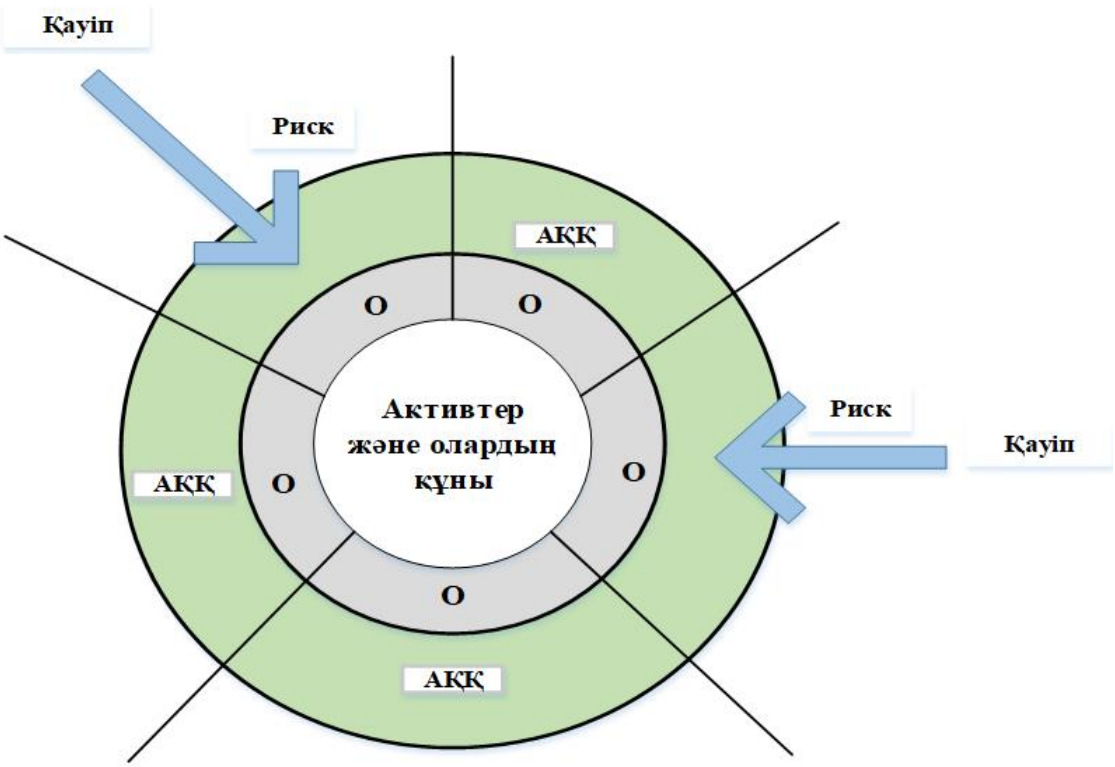
1.3-сурет. Заңды тұлғаларға жасалған кибершабуылдар нәтижесінде ұрланған деректердің түрлері (2018-2022)



1.4-сурет – 2018-2022 жылдардағы компаниялар мен кәсіпорындардың кибернетикалық қауіп-қатерлерге шабуыл түрілері



1.5-сурет – 2018-2022 ж. экономика салалары бойынша кибершабуыл құрбандарының санаты



О – осалдық; АҚҚ – ақпаратты қорғау құралдары

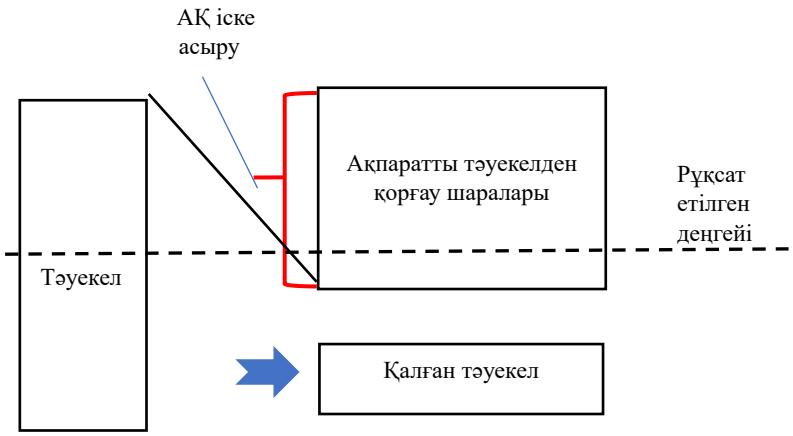
1.6-сурет – Ақпараттық қауіпсіздік элементтерінің өзара байланысы

1.7-суретті АҚ шаралары мен тәуекелдердің өзара байланысының моделі. Іс жүзінде тәуекелдерді тиімді деңгейге дейін төмендету үшін бірнеше АҚ шараларын қолдану қажет. Тәуекелді азайту үшін кейбір қорғаныс шараларының тиімділігін көрсететін қорғаныс шаралары мен тәуекелдің өзара байланысы 1.7-суретте көрсетілген. Егер тәуекел тиімді деп саналса, қорғаныс шараларын жүзеге асырудың қажеті жоқ, сондықтан қорғаныс тараптарының ресурстарын қайта бөлудің де қажеті болмайды.

Жоспарлау кезеңінде АҚ және тәуекел шараларының өзара байланысы моделі: тәуекелдерді бағалауды; АКЖ АҚ жоспарын әзірлеуді көздейді. Жоспарлаудан кейін келесі кезең АҚ шараларын іске асыру болып табылады. АҚ шаралары мен тәуекелдің өзара байланысы моделінің негізгі қағидаттары: қалдық тәуекелдерді тиімді деңгейге дейін азайту мақсатында АҚ-ның бірнеше шаралары бір мезгілде қолданылуы мүмкін; қалдық тәуекелдің тиімді деңгейі жағдайында АҚ шараларының саны азаюы мүмкін.

АҚ АҚО саясаты АҚ қағидаттарынан және тұтастай алғанда ұйымның (компанияның, кәсіпорынның) директиваларынан тұруы мүмкін. Кейбір жағдайларда ол техникалық немесе басқару саясатына қосылуы мүмкін. Бұл саясаттар жиынтығында АҚ саясатының негізін құрайды.

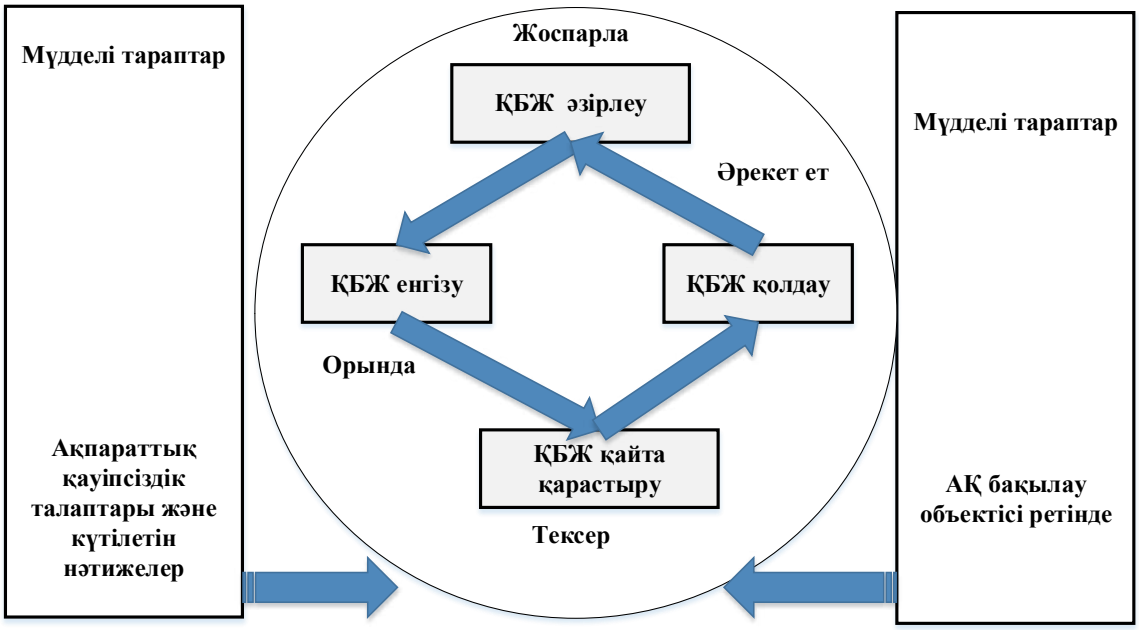
Корпоративтік АҚП иерархиясы моделінің негізгі қағидаттары: корпоративтік АҚП тұтастай алғанда ұйым үшін қорғау қағидаттары мен директиваларды қамтуы мүмкін; АҚП қауіптерге әлсіз немесе ұйым үшін ерекше маңызы бар өте құнды АҚ-ға қатысты қағидаттар мен директиваларды қамтуы мүмкін; АҚ-ның АКЖ саласындағы корпоративтік саясаты АҚ-ның негізгі қағидаттары мен АҚ-ның корпоративтік саясатына және АКЖ-ны АҚО-да пайдалануды реттейтін жалпы бизнес-процестерге қатысты директиваларды көрсетуі тиіс; АКЖ АҚ саясаты АКЖ-ны пайдалану саласындағы АҚ корпоративтік саясатында қамтылған АҚ қағидаттары мен нұсқамаларды көрсетуі тиіс; ол, сондай-ақ, іске асырылатын АҚ-ның нақты талаптары мен кепілдіктері туралы ақпаратты қамтуға тиіс.



1.7-сурет – АҚ шаралары мен тәуекелдердің өзара байланысының моделі

Басқару түрлерінің, АҚО өлшемдері мен құрылымдарының айырмашылығы процестің қоршаған ортаға бағдарын тудырады.

«Жоспарла – орында – тексер – әрекет ет» моделі (1.8-сур.) бұдан әрі барлық АҚБЖ- ға қолданылады (кейбір авторларда АҚ қамтамасыз ету жүйесі немесе АҚОЖ [12, б.76]). Ол АҚБЖ (АҚОЖ) регламенттелген процестердің көмегімен мүдделі тараптардың талаптары мен болжалдарына – кіріс деректеріне сәйкес келетін АҚ шығыс деректерін қалай жүргізетінін суреттейді.



1.8-сурет – «Жоспарла - орында – тексер - әрекет ет" АҚ моделі

«Жоспарла – орында – тексер – әрекет ет» моделіне сәйкес АҚО АКЖ АҚ басқару кезеңдерінің мазмұны 1.1-кестеде келтірілген.

Қорғаныс ресурстарын динамикалық басқару және шабуылдаушы тарапқа белсенді қарсы тұру, сондай-ақ АҚ және КҚ тәуекелдерін басқару процесін құру кезінде ISO/IEC 17799, ISO/IEC 27001 және CobiT (Control Objectives for Information and related technology), сонымен қатар NIST (National Institute of Standards and Technology) халықаралық стандарттарының ережелері мен талаптарын ескеретін әдістер қолданылады [13, 14].

Сондай-ақ бірқатар авторлардың зерттеулері мен тәжірибелері [15-17] негізінде әзірленген бірегей әдістемелер, сондай-ақ әлемдік практика мен халықаралық стандарттар, жүйелік талдау мен жобалаудың құрылымдық әдістеріне негізделген арнайы аспаптық құралдар (SSADM-Structured Systems Analysis and Design) пайдаланылады.

Бүгінгі таңда АКЖ және олардың АҚҚ-ге қойылатын ең маңызды тұжырымдамалық талап - икемделу талабы [18]. Мұндай қызметке АҚҚ нақты ұйымдастыруға және тұрақты басқаруға негізделуі керек. АКЖ-дағы басқару деп оның жұмыс істеуінің әр кезеңінде жүйенің элементтеріне мұндай бақылау әсерін анықтау деп түсініледі, нәтижесінде бір немесе бірнеше функционалды есептерді шешуге болады. Функционалдық есептер деп АТЖ іске асыратын

функционалдық қатынастағы біртекті операциялар жиынтығын айтады [18, 129-б.]. Қазіргі заманғы компьютерлік техниканың даму деңгейі АҚ-ны басқарудың тиімділігін арттыру және автоматтандыру үшін АКЖ қауіпсіздігін басқару орталығында қолданылатын шешім қабылдауды қолдаудың ішкі жүйелерін АҚҚ құрамына қосуға мүмкіндік берді.

АҚҚ декомпозициясының нәтижесінде үш ұйымдастыру бөлігін бөлуге болады: АҚ қамтамасыз ету тетіктері; АҚ механизмдерін басқару механизмдері; Жүйе жұмысын жалпы ұйымдастыру тетіктері.

1.1-кесте – «Жоспарла – орында – тексер – әрекет ет» моделіне сәйкес АОБ АКЖ АҚ басқару кезеңдерінің мазмұны

№	Кезең	Тапсырма
1	**АҚБЖ ЖОСПАРЛАУ** (әзірлеу)	Жалпы АҚО саясаттары мен мақсаттарына сәйкес келетін нәтижелерге қол жеткізу үшін тәуекелдерді басқару және АЖ жақсарту үшін маңызды АҚБЖ саясатын, мақсаттарын, процестерін және процедураларын әзірлеу.
2	**АҚБЖ (АҚОЖ) ОРЫНДАУ** (енгізу және жұмыс істеуін қамтамасыз ету)	АҚП жұмыс істеуін енгізу және қамтамасыз ету, АҚБЖ процестері мен рәсімдерін бақылауды жүзеге асыру.
3	**АҚБЖ-ны ТЕКСЕРУ** (мониторингті және қайта қарауды (түзетуді) жүзеге асыру)	АКЖ процестерінің өнімділігін АҚБЖ саясатына, мақсаттарына және практикалық тәжірибесіне сәйкес бағалау және мүмкіндігінше өлшеу. Қажет болған жағдайда АҚБЖ-ға түзетулер енгізу үшін басшылыққа нәтижелер туралы есеп беру.
4	**ӘРЕКЕТ** (АҚБЖ қолдау және жетілдіру)	АҚБЖ-ны тұрақты жетілдіруге қол жеткізу үшін, оның ішінде қорғау ресурстарын динамикалық түрде қайта бөлу қажет болған жағдайлар үшін АОБ-ның басшысы, АҚ қызметтері немесе басқа да маңызды ақпарат тарапынан АҚБЖ-ны ішкі аудит және қайта қарау нәтижелері негізінде түзету және алдын алу іс-шараларын пайдалану.

Қарсы қорғаныс шараларының бірі – ресурстарды бейімделме басқару. Бұл ретте ресурстарды бөлу қорғаныс тарабы үшін нақты шабуылдың мақсатын анықтау қажеттілігінен туындаған кідіріспен жүргізіледі [19]. Осылайша, қорғаныс ресурстарын динамикалық басқару есептерінде шешімдерді қолдау үшін әдістерді, модельдерді және сәйкес алгоритмдерді әзірлеу есепсі туындайды. Мұнда, әзірленген шешімдер үнемі өзгеріп отыратын жағдайларда қорғаныс жағы үшін ұтымды көрсеткіштерге қол жеткізуді қамтамасыз етуі керек. Ойын теориясының терминологиясын қолдансақ, онда позициялық

ойынмен істес боламыз. Сол кезде жоғарыда айтылғандарға сәйкес бірқатар сұрақтар туындайды:

1) осы ойында мақсатты функциямен анықталған мән үшін ершік нүктесі қандай жағдайда болады және оның жағдайына қарсы тұру шарттары қалай әсер етеді: шабуыл (*H*) және қорғаныс (*D*) ресурстарының салыстырмалы саны, (*Z=H/D*) объектілер(*k* - объект нөмірі), объектілердің әлсіздігі $\{V_k\}$ арасында АР бөлу $\{g_k\}$;

2) ершік нүктесі болмағандағы белгісіздік жағдайында қорғау ресурстарын бөлу $\{d_k\}$ қандай болуы тиіс;

3) шабуылдардың бағыттылығы белгілі болған жағдайда, жалпы шығындар ең аз болатындай етіп, әртүрлі әлсіздігі бар объектілер арасында АР-ды $\{g_k\}$ қайта бөлу қалай болады;

4) келесі шамаларды айқындайтын ұтымдылықтың әртүрлі критерийлерін және әртүрлі мақсат функцияларды пайдалану кезінде басқару алгоритмдері қалай ерекшеленеді: жоғалған АР саны; АР инвестицияларынан түсетін пайда; АР рентабельділігі; және көп мақматты функцияны пайдалану кезінде нәтиже қандай болады;

5) тараптардың әрқайсысы өз ақпаратын қорғауға арналған ресурстардың бір бөлігін, ал екіншісін қарсыластың іс-әрекеттері туралы ақпарат алуға жоғалтқан кезде кешенді қарсыласуда басқару алгоритмі қандай болады.

АҚ және КҚ менеджментінің математикалық модельдерінде көрсетілгендей [20-22], мақсатты функция, әдетте, белгілі бір дәрежеде АҚ жүйесінің (бұдан әрі – АҚҚ) әлсіздігі арқылы қарсыласу көрсеткіштерінің бірін (көбінесе оның ұтымды мәнін) айқындайды. Мысалы, Гордон-Лоеб моделінде (ГЛ) [23] бұл көрсеткіш АҚҚ-ге инвестиция салу арқылы АР жоғалуынан болатын шығындардың азаюы болып табылады. Өз кезегінде, Қорғаныс объектісінің әлсіздігі, егер қорғаныс шығындары нөлге тең болса, шабуылдың сәтті болу ықтималдығы ретінде қарастырылады.

Соңғы онжылдықта ақпараттық қауіпсіздік есебін сипаттайтын кем дегенде ондаған модель пайда болғанын ескертеміз. Ең көп тарағаны – Гордон-Лоеб моделі (ГЛ) [24]. Бұл модельдің мақсаты ақпаратты қорғауға инвестициялардың ұтымды мөлшерін анықтау есебін шешу болып табылады. Модельдің басты ерекшелігі - АҚ деңгейін анықтайтын әлсіздік функциясын енгізу және дамыту.

1.2-кестеде ұқсас модельдер мен олардың нұсқаларының өте көп екенін ескере отырып, АОБ АҚ басқаруды ұтымды шешу саласындағы барлық қызықты және сұранысқа ие модельдер жүйеленген, сонымен қатар олардың күшті және әлсіз жақтары келтірілген.

1.2-кесте – АОБ АҚ басқаруды ұтымды шешу саласындағы модельдер. [23-36] материалдар бойынша құрастырылған.

№	Модельдің қысқаша сипаттамасы	Артықшылық тары	Кемшіліктері
1	2	3	4
1	**Гордон-Лоеб моделі** [23]**.** ГЛ моделіндегі басты нәрсе – АҚ деңгейін анықтайтын әлсіздік функциясын енгізу және әзірлеу. Негізгі параметрлер: ақпараттың жайылып кетуінен болатын ықтимал шығындар; шабуыл жасау ықтималдығы; АР әлсіздігі; АҚ-ға арналған шығындар; шабуыл нәтижесінде болатын шығындар ықтималдығы; АҚ-ға инвестициялар болмаған кездегі ықтимал шығындар; АҚ және КҚ бұзу ықтималдығы.	Алғаш рет қорғаныс пен шабуыл арасындағы қарама-қайшылықты қарастыруда маңызды болып табылатын әлсіздік функциясы анықталды.	Құрылымы бойынша модель статикалық болып табылады. Шешімдер мен нәтижелер бір уақытта шығады, ал динамикалық әсерлер ескерілмейді.
2	**Гросс моделі.**[25]**.** Модельге сәйкес, қақтығысушы тараптардың ресурстары $(D),(H)$ бар және олардың қарсыласу нәтижесі мақсатты функциямен анықталады, ол салынған ресурстардың айырмашылығына сызықты тәуелді болады және сызықты бағдарламалау есебіне әкеледі. Негізгі параметрлер: $k-$ объектідегі шабуыл және қорғаныс ресурстары, объектілердің маңыздылығын немесе олардың әлсіздігін білдіретін салмақ коэффициенті.	Модельдің қарапайымдылығы.	Модельдің басты кемшілігі – оның мақсатты функциясының сызықты сипаты. Бұл шынайы жағдайларға сәйкес келмейді. Гросс моделін оның қарапайымдылығын ескере отырып, тек мақсатты функцияны жуықтату және алғашқы жуықтауда нәтиже алу үшін пайдалануға болады.

1.2-кесте жалғасы

	2	3	4
3	**Задирак В.К. моделі** [26]**.** Модельде мақсатты функция ақпараттың жайылып кетуінен болатын шығындар мен оны қорғау шығындарының мөлшерін анықтайды. Жағдайды сипаттайтын теңдеулер жүйесін шешу ақпаратты қорғауға арналған мақсатты шығындарды ұтымды шешуге сәйкес келетін шамалар үшін мәндер кестесін алуға мүмкіндік береді.	Модельдің қарапайымдылығы.	Шабуыл тарапының ресурстары ескерілмейді. Динамикалық режимдегі ұтымды шешім есебі жоқ.
4	**Фомченкова Л.В. моделі** [27]**.** Ұйымның ақпараттық қауіпсіздігімен байланысты ішкі қауіптер мен тәуекелдердің біріктірілген идентификаторы негізінде, сондай-ақ сандық әлеуетті, бизнесті және АТ стратегияларын ескере отырып, АҚ басқару саласындағы шешімдерді қалыптастыруға, қажетті ақпараттық қорғаудың дәрежесі мен әдісін анықтауға мүмкіндік береді.	Ұйымдағы АҚ бақылау функциялары на бағытталған.	Модель тәуелсіз емес. Оны қолдану үшін қосымша басқа әдістер мен модельдерді, атап айтқанда, қауіптердің әрқайсысының әсер ету дәрежесін сипаттау үшін пайдалану қажет. Модель шабуыл тарапының ресурстарын ескермейді. инамикалық режимдегі ұтымды шешім есебі жоқ.

1.2-кесте жалғасы

1	2	3	4
5	**Калашников А. О. моделі** [28]**.** Модель сыни инфрақұрылымның АҚ-ны басқарудың кейбір аспектілерін оның ауытқыған күйлерін анықтау негізінде сипаттайды. Кешенді бағалау, жүйелік және кластерлік талдау алгоритмдері қолданылады.	Кластерлік талдау алгоритмдерінің арқасында объектілерді қарастырылатын объектілердің түріне ешқандай шектеулер қоймай, бірқатар белгілерге сәйкес бөлуге болады.	Модель жүйеде ауытқулар туралы статистика болған жағдайға ғана бағытталған. Шабуыл тарапының ресурстары есепке алынбайды. Динамикалық режимдегі ұтымды шешім есебі жоқ.
6	**Котенко И.В. моделі** [29, 30]**.** АҚ басқарудың зияткерлік тетіктерін іске асыруға негізделген. КҚ-ны басқару ақылды агенттер, шабуылдаушының жалған ақпарат беру механизмдері, жасыру және камуфляжға негізделген.	Модельдің кешенділігі	Жоғары есептеу күрделілігі. Динамикалық режимде модельді және есептеу нәтижелерін қолдануға арналған параметрлер жоқ.
7	**Глушак, В. В., Новиков және Архипов модельдері** [31-34]**.** Модель тәуекелдің ықтималды параметрлерін анықтауға арналған. Жағдайды сипаттау үшін: шабуылдаушының қауіп-қатерді жүзеге асыру шығындары; шабуылдаушының алған «ұтысы», қорғаныс тарапынан келтірілген залал.	Модельдердің көрнекілігі.	Қорғаныс объектілері арасында ресурстарды бөлуді ұтымды шешу есебі қарастырылмады.
8	**Ахметов-Лахно -Малюков модельдері** [35]**.** Модельдер ойын теориясының негіздеріне құрылған және қорғаныс пен шабуыл ресурстары арасындағы қарама-қайшылық контекстінде жағдайды қарастырады.	Модельдер қорғаныс тарапының қаржылық стратегияларын таңдауды ұтымды шешу қажет болған барлық жағдайларды қамтиды.	Модельдердің есептеу күрделілігі жоғары. ШҚҚЖ қолданбай есептеу өте қиын

Ресурстарды басқаруды математикалық модельдеу саласындағы ғылыми жұмыстарды талдау ақпаратты қорғау тараптары негізгі күш-жігердің қорғауға салынған инвестициялар көлемін анықтауға бағытталғанын көрсетті (1.1-кесте.). Бұл инвестицияларды қорғау объектілері арасында бөлу есептеріне жеке зерттеулер ғана арналған. Сонымен қатар, қолданыстағы әзірлемелер шабуылдаушының ықтимал әрекеттері мен олардың салдарының АОБ-дағы АЖ көрсеткіштері мен сипаттамаларының өзгеруіне әсерін сирек ескереді.

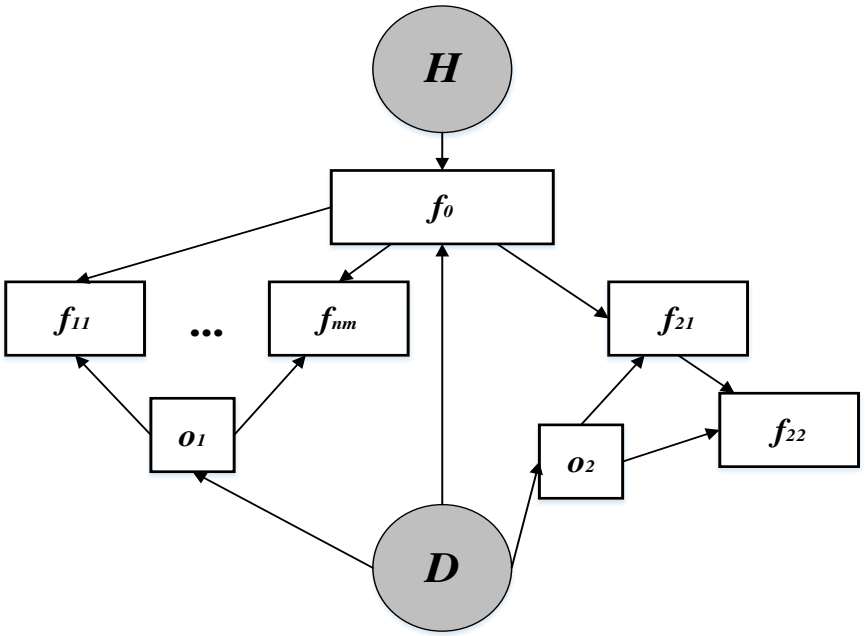
Жоғарыда келтірілген ғылыми жұмыстарды талдау нәтижесінде шаруашылық қызмет субъектілерінің ақпаратын қорғауға бөлінетін шектеулі қаржы ресурстарын тиімді пайдалану есебі барған сайын маңызды бола түсуде және айтарлықтай дәрежеде кез келген мемлекеттің АҚ және КҚ деңгейін айқындайды [36]. Сонымен қатар, белгісіздік жағдайында, шабуылдаушы тараптың әрекеттерінің дәйектілігі алдын-ала белгісіз және белгілі бір ықтималдықпен ғана мақсатты шабуыл сценарийін болжауға болатын кезде, теориялық-ойын әдістерін қолдану және қарама-қайшылық жағдайларының өзгеру динамикасын ескере отырып, АҚ объектілері арасында шектеулі ресурстарды ұтымды бөлуді іздеу қаржылық шығындарды ақпараттық ресурстардың жайылып кетуінен азайтуға мүмкіндік береді.

АҚ және АОБ КҚ саласындағы көптеген зерттеулер көрсеткендей, ақпараттың көлемі мен құнының өсуі АҚҚ тиесілі қиындауына алып келеді. Қазіргі заманғы АҚҚ көп деңгейлі және көп контурлы болып келеді.

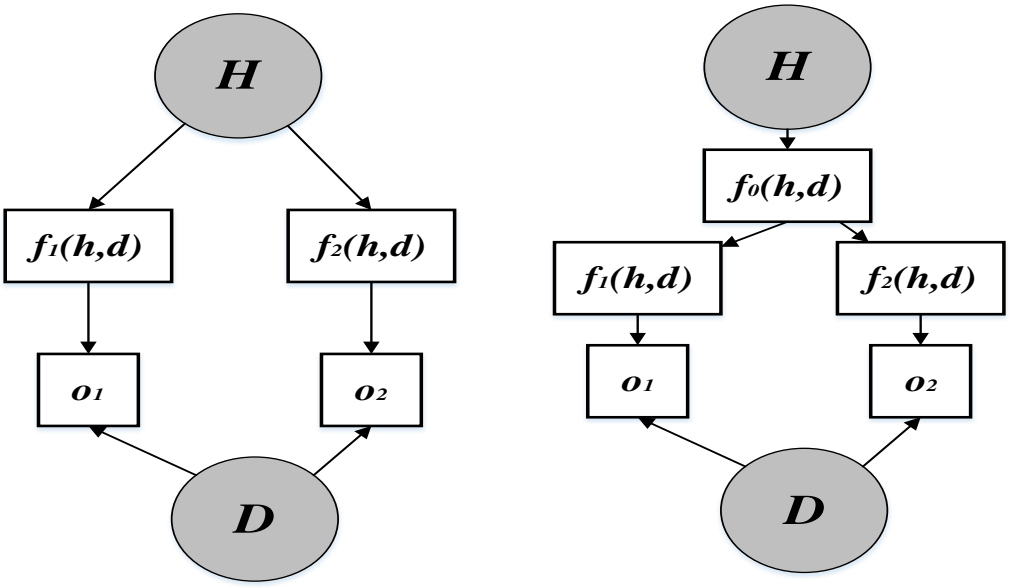
АҚҚ құнының өсуі қорғау ресурстарын ұтымды пайдалану есебін өзекті етеді. Шешімдерді іздеу процесінде уақыт өте келе шабуылдаушы тараптың қарсыласу жағдайларының өзгеруін ескеру қажет. Бұл ақпараттық ресурстардың «қартаюына», олардың жаңаруына, жаңа шабуыл құралдарының пайда болуына, АҚҚ модернизациясына және т.б. байланысты. Нәтижесінде, біз күрделі қорғаныс құрылымдарындағы ресурстарды динамикалық басқару есебін шешу қажеттілігіне тірелеміз.

1.9-суретте мұндай құрылымның мысалы көрсетілген. Схема физикалық және электронды жүйелерді сипаттайды. Физикалық жүйенің мысалы f_0 шабуылдаушылар үшін жалпы кедергі аумақтың қорғалған периметрі болатын жүйе болуы мүмкін. Үй-жайдың o_1, o_2 – объектілері, ал f_{ij} – тиісті үй-жайларды қорғауға арналған құралдар. Мұнда i, j – индекстер, сәйкесінше, объектінің нөмірі, кедергі нөмірі болып табылады.

Бірінші объектінің f_{11}, f_{12}, f_{13} параллель қорғаныс құралдары, мысалы, электр және жылу желілерін жерге қосу, экрандау, үй-жайларды шулату. Екінші объектінің f_{21}, f_{22} бірізді қорғаныс құралдары іргелес бөлмелерде орналасқан. Электрондық жүйеде (1.9-сурет.) o_1, o_2 – объектілер – жалпы және жеке қорғаныс құралдары бар компьютерлер, серверлер. Мысалы, жалпы қорғаныс – бұл firewall. Тиісінше, жеке қорғаныс - бұл антивирустық БҚ. Күрделі схеманы (1.9-сурет) декомпозиция әдістерімен қорғаныс элементтерінің параллельді (1.10, а-сурет) немесе тізбекті-параллельді (1.10, б-сурет) орналастырып, қарапайым схемаларға (1.10-сурет) келтіруге болады.



1.9-сурет – АОБ үшін АҚҚ құрылымы



а) б)

а – АОБ үшін бір деңгейлі АҚҚ;
б – АОБ үшін екі деңгейлі АҚҚ
1.10-сурет – АОБ үшін жеңілдетілген АҚҚ схемалары

Көп тізбекті қорғаныс жүйелерінде ақпаратты қорғау ресурстарын бөлудің негізгі заңдылықтарын анықтау үшін жеңілдетілген құрылымдарды қарастырумен шектелуге болады (1.10-сурет.). Сонда, мысалы, кедергілердің

бірізді-параллель орналасуын талдау (1.10-сурет, б) арқылы, келесі есептерді жеке немесе жиынтықта қарастыруға болады:

(1.10-сурет, б) схема мен (1.10-сурет, а) схеманы салыстыру және ақпаратты қорғау тарапының бюджеті өзгермеген кезде қорғаудың қосымша элементін (кедергілер немесе бөгеуілдер) енгізудің орындылығын айқындау; қорғаудың жалпы элементтері (мысалы, файервол, қолжетімділікті бақылау жүйесі және т. б.) мен жеке қорғаныс құралдары (мысалы, вирусқа қарсы бағдарламалар, криптографиялық қорғау құралдары және т. б.) арасында ресурстардың ұтымды бөлінуін анықтау; қорғаныс ресурстарын бөлу схемаларының әртүрлі нұсқалары мен комбинациялары арасындағы корреляцияны зерттеу. Соңғысы ұтымды схеманы таңдау үшін орындалады; АОБ үшін көп контурлы АҚҚ-да ресурстарды басқару бойынша ұсыныстар әзірлеу.

АОБ ақпараттық инфрақұрылымын талдау жоғарыда қарастырылған АҚ және КҚ бағалау және басқару әдістемелерінің (1.1-кесте.) кез келгенінің есепті кезеңі екенін ескертеміз. Бұл талдау неғұрлым терең болса, бағалау нәтижесі соғұрлым объективті болады. АОБ ақпараттық инфрақұрылымын талдау кезінде, сондай-ақ АОБ АЖ тағайындалуын; АЖ мен оның АҚҚ функционалдық талаптарын; АЖ мен деректердің сыни болуын; АОБ желісінің ағымдағы топологиясын; жүйелік интерфейстерді; ақпараттық ағындарды; АОБ персоналын; енгізілген қауіпсіздік саясатын; АЖ үшін техникалық бақылау құралдарын және т. б. ескеру қажет. Осылайша, тиімді АҚҚ құру үшін кешенді түрдегі және оның тиімділігін анықтайтын көрсеткіштердің жеткілікті үлкен санын ескеру қажет. Сонымен қатар, олардың талаптарының сәйкес келмеуіне байланысты әртүрлі көрсеткіштердің ұтымды мәндеріне қол жеткізу өте қиын және көбінесе мүмкін емес [37, 90-91 бет]. Нәтижесінде, біз көп критерийлі тапсырмаға тірелеміз. Мұндай есепті шешу әрқашан жеке көрсеткіштердің талаптарын қанағаттандыруда ымыраға келу болып табылады. Мұндай көп критерийліесептерді шешкен кезде әрқашан шешім алгоритмдерін таңдау дилеммасы болады. Егер мұндай әдістер мен алгоритмдерді жалпыласа, оларды екі тәсілге дейін азайтуға болады – анық және анық емес. Бұл жіктеуді жеткілікті түрде шартты деп санауға болады. Бұл, әсіресе, ақпаратты қорғауға байланысты есептерге қатысты, өйткені қорғау тарапының әрекеттері көбінесе белгісіздік жағдайында болады. Тиісінше, есептің тұжырымы және нәтижелері дәл болуы мүмкін емес. Егер нақты көзқараспен объективті функцияның экстремалды мәні оның сарапануына қатысты кейбір шарттарды орындау кезінде бар және оны табуға болатын болса, онда түсініксіз жолмен жеткілікті түрде хабардар болмау шешімге қод жеткізуге мүмкіндік бермеуі ықтимал, ал АОБ-ны қорғаудың мақсаты берілген шектеулермен жеткілікті түрде орындалмауы мүмкін.

1.2. Ақпараттандыру объектілерінің киберқауіпсіздік ресурстарын көп критерийлі ұтымды шешу мен динамикалық басқарудың математикалық әдістерін талдау

Кез келген процестерді немесе құбылыстарды жетілдіру әрқашан оларды сипаттайтын өлшемдерді анықтауға негізделген. Бұл өз кезегінде зерттелетін процестерді немесе құбылыстарды ұтымды шешуды қамтамасыз ету жолдарын қалыптастырудың жеткіліктілігінің алғышарты болып табылады.

Қазіргі заманғы АҚҚ – өте күрделі құрылымдар, 1.11-суретті қараңыз. Мұндай көп контурлы жүйелерде АҚҚ ақпараттық ресурстарының тұтастығын, құпиялылығын және қол жетімділігін қорғау үшін жергілікті есептерге жауап беретін көптеген объектілері болады. АОБ өмірлік циклі бойында аппараттық, бағдарламалық, ұйымдастырушылық құралдар мен қорғаныс әдістерінің әртүрлі конфигурацияларын қамтуы мүмкін мұндай көп контурлы жүйелерді зерттеу қиын есеп болып табылады. Әдетте, мұндай көп контурлы АҚҚ-ны жобалау немесе модернизациялау кезеңінде қорғаныс құралдарының құрамын көп критерийлі ұтымды шешуге байланысты есептерді шешу қажет. Бұл жағдайда қорғаныс ресурстарын динамикалық басқарудың аспектілерін ескеру керек. Мұндай көп критерийлі есептерді, ең алдымен, математикалық модельдеудің әртүрлі әдістерін қолдану және АОБ көп контурлы қорғаныс кешендерінің құрамын көп критерийліұтымды шешу арқылы шешу керек.

Бұл жағдайда мұндай көп критерийлі ұтымды шешу есептерін шешудің математикалық модельдері екі қарама-қайшылықты талаптарға жауап беруі керек:

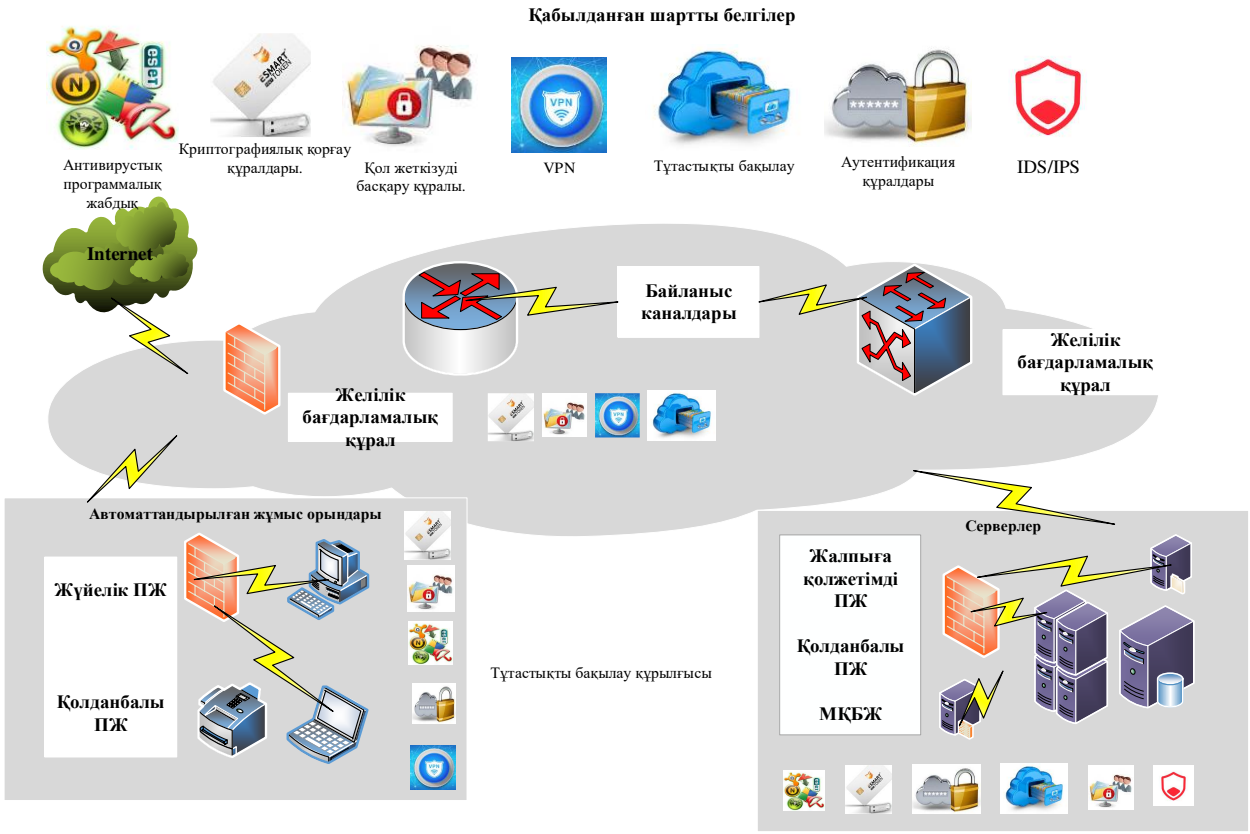
1) жүйенің қасиеттерін барынша көрсету;

2) бұл ретте түпкілікті нәтиже алуды қиындатуы мүмкін артық бөлшектенуден аулақ болуға тиіс.

Сондай-ақ, келесі жағдайды ескеру қажет. АОБ қорғаныс жағының динамикалық ресурстарын басқару есеплері бұл тек АОБ киберқауіпсіздік контурындағы қорғаныс компоненттерінің санын көбейту арқылы шешілетін таза техникалық есеп емес. Бірақ бұл басқарушылық есеп те. Сонымен қатар, екінші есеп АҚ және КҚ менеджменті сияқты ұғыммен байланысты [37]. АҚ және КҚ менеджментінің негізгі есебі АОБ үшін АҚҚ жұмыс істеу тиімділігінің техникалық ғана емес, экономикалық көрсеткіштерін де ұтымды шешу болып табылады.

АҚ саласындағы ресурстарды ұтымды бөлу есебін зерттеуге АОБ үшін шетелдік ғалымдардың да, Қазақстан Республикасының ғалымдарының да көптеген жұмыстары арналған. Осы саладағы зерттеу тақырыбы өзекті және әртүрлі халықаралық ғылыми конференцияларда сұранысқа ие [38-40].

Осылайша, [41] жұмыста АКЖ АҚ шығындарын ұтымды шешу есептері талданды. Негізінде көп критерийлітаңдау есебін шешу туралы сөз болады. АОБ үшін АҚҚ-ға шығындарды бөлудің ұтымды нұсқасын таңдаудың интерактивті процедурасы ұсынылды.



1.11-сурет – ISO/IEC 27001 талаптарына сәйкес барлық компоненттердің шартты белгілері бар ақпаратты қорғаудың көп контурлы жүйесінің схемасы

[42] жұмыста АОБ үшін АҚ және КҚ қамтамасыз ететін механизмдерді басқарудың әртүрлі функциялары арасында ресурстарды ұтымды бөлу есебінің алты түрлі тұжырымы келтірілген. АҚ-ны қамтамасыз ететін жүйелерді жобалау сатысында да, АҚ контурларын жетілдіру және дамыту кезеңдерінде де қолдануға арналған ресурстарды бөлу есебін қою ұсынылады. Авторлар АҚ-ны қамтамасыз етудің жеті негізгі функциясын анықтайды [42, 113-б.] және әртүрлі АҚҚ функциялары арасында қаражат бөлудің бөлшектеуге және рәсімдеуге арналған екі тәсілін ұсынады. Бірінші тәсіл АҚ қаражатының құрамы мен санын есепке алуға негізделген. Екінші тәсіл жалпыланған заңдылықтарды талдауға және АОБ-ны АҚ құралдарымен қамтамасыз ету процесіне енгізілген қатынастар мен оларды қолданудың тиімділігіне негізделген. Жұмыста ықтимал және шығындар модельдері қарастырылған. Соңғысы зерттеушілер үшін үлкен қызығушылық тудырады, авторлар ұсынған бағдарламалық өнімге деректерді енгізу кезінде ресурстарды бөлу есебі параметрлерінің физикалық мағынасын нақтылайды.

[43] жұмыста АҚҚ объектілері арасында ресурстарды бөлуді ойын моделі және объектілердің тең қауіпсіздігі қағидаты негізінде орындау ұсынылатын модель қарастырылады. Ресурстарды бөлу есебі екі ойыншы - қорғаушы және нөлдік шабуылшы турнирі ретінде тұжырымдалған. Әр ойыншы басқа ойыншының бекітілген шешімімен сызықтық бағдарламалау есептерін шешеді. Жұмыста кепілдендірілген нәтиже алу үшін дәйекті түрде қолдануға болатын үш алгоритм ұсынылған. Алгоритмдер математикалық негізделген, нәтижелер тест мысалдарымен расталған және жалпыланған. АОБ АҚ арттыруға

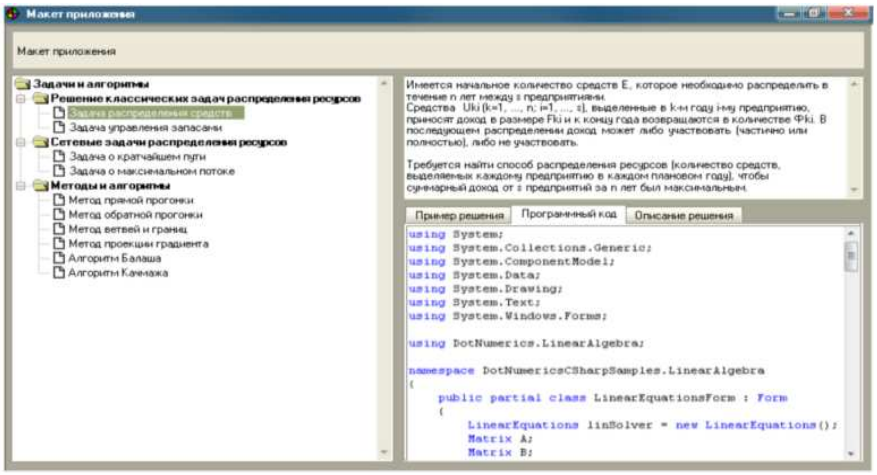
бағытталған қаржы ресурстарын бөлудің ойын модельдері де жұмыста егжей-тегжейлі қарастырылған [44, 45].

Белгілі бір математикалық әдістерді жүзеге асыратын БҚ көпшілігі дайындалған кірістерге байланысты көптеген есептерді шешуге мүмкіндік беретін өте әмбебап өнімдер болып табылады. [46] жұмыста сипатталған бағдарламалық пакеттің басты ерекшелігі - есептеу операциялары мен жұмыс уақытының өлшемі бойынша ең тиімді алгоритмді таңдауға мүмкіндік беретін ақылды агенттің болуы. Сонымен қатар, АҚҚ құру кезінде АҚҚ-ның ұзақ мерзімді функционалдығын қамтамасыз ететін ресурстардың уақтылы бөлінуі де ескерілетіні өте маңызды. [46, 87-б.] жұмыста АҚҚ-ға бөлінетін ресурстарды бөлу есептерін шешу үшін БҚ сипатталған, 1.12-суретті қараңыз.

ШҚТ-ның жүйемен жұмысы «бұлтты» сервисте есепті шешу үшін құралдарды орналастыру талаптарын ескере отырып, online-режимде өтеді. Бұл пайдаланушыға қажетті БҚ-ны және оны орнатуды іздемей, есептің шешімін табуға мүмкіндік береді.

Пакетке енгізілуі керек әдістерді таңдау кезінде зерттеу тапсырмасын орындау, тапсырманың түрін анықтау және сәйкесінше кіріс деректерін дайындау қажет болды. АҚҚ-да ресурстарды бөлуді модельдеу есебін шешу үшін бағдарламалық пакеттің прототипіне енгізілген бөлімдердің тізімі: ресурстарды бөлудің классикалық есептерін шешуге арналған бөлім (кәсіпорындар арасында ресурстарды бөлу және қорларды басқару есептері); ресурстарды бөлудің желілік есептерін шешуге арналған бөлім (ең қысқа жолды табу және ең жоғары ағын туралы есептер);қолданбалы есептерді шешуге арналған бөлім (қатерлердің кейбір түрлерін жою есебінен ақпараттық қауіпсіздік тәуекелдерін төмендету мақсатында қаржы ресурстарын бөлу есебі енгізілген); әдістер мен алгоритмдерден тұратын бақылау бөлімі (шартты ұтымды шешу әдісі, бұтақтар мен шекаралар әдісі, алға және кері жүгіру алгоритмдері, Качмаж және Балаш алгоритмдері, генетикалық алгоритмдер және т.б.).

1.12-сурет – Ресурстарды бөлудің ұтымды нұсқаларын, оның ішінде ақпаратты қорғау жүйелеріне бөлінетін шешімдерді қабылдауды қолдау жүйесінің макеті



Өкінішке орай, бұл әзірлеме макет түрінде болып қалды және зерттеу жұмысы авторлары оны аяғына жеткізе алмады. Қарсыласу сценарийлерінің күрделенуі жаңа жағдайлар мен туындаған жағдайларды көрсетуі керек математикалық модельдердің құрылымында көрінеді.

Көп критерийлі ұтымды шешу есептерін қалыптастыру және оларды шешу әдістерін әзірлеу тарихқа бай. Диссертацияның осы бөлімі аясында мұндай есептерді шешудің барлық әдістері мен модельдерін егжей-тегжейлі сипаттамай, біз барлық белгілі әдістерді жүйеледік.

1.3-кестеде АОБ үшін АҚ және КҚ көп контурлы жүйелерінің ұтымды конфигурацияларын табу есебін шешу үшін көп критерийліұтымды шешу әдістерінің салыстырмалы сипаттамасы келтірілген.

1.3-кесте – АОБ үшін АҚ және КҚ көп контурлы жүйелерінің ұтымды конфигурацияларын іздеудің көп критерийліұтымды шешу есептерін шешу әдістерін салыстырмалы талдау. [47-59] материалдар бойынша жасалған

№	Әдіс	Артықшылықтары	Кемшіліктері
1	2	3	4
1	Парето бойынша ұтымды шешімдер алу негізінде көп критерийлі келісімді қалыптастыру [47].	Әдісті практикада қолдану көп критерийліұтымды шешудің басқа әдістерімен салыстырғанда ең қарапайым болып табылады.	Зерттелетін параметрлердің маңыздылық деңгейін анықтау қиын. Ол үшін сарапшылардың сауалнамалары қолданылады, сондықтан бұл әдісті қолдану нәтижесі олардың субъективті сенімдеріне байланысты болуы мүмкін.
2	Барлық басқа критерийтардың салмағын азайта отырып, бірнеше критерийтарды бір скаляр параметрге біріктіру [48].	Алынған параметрге жеке критерийтар тобының әсерін зерттеу қажет есептерді шешу үшін қолдануға болады.	Ұтымды шешімдерді іздеу ұтымды келісімге қол жеткізуге қандай критерийтар әсер ететіні белгісіз болғандықтан қиындайды. Сонымен қатар, скаляр параметрінде критерийтарды өлшеу әдістерін анықтау қиын. Басқа критерийтардың салмағын азайту деңгейін анықтау қиын.

1.3-кесте жалғасы

1	2	3	4
3	Өлшенген сомалар әдісі (басқалардың салмағын азайтпай бірнеше зерттелетін критерийтарды біріктіру) [49].	Бұл әдісті бірнеше критерийтар бірдей мәнге ие есептерді шешу үшін қолдануға болады.	Әдісті қолдану нәтижесі есепті түрде ұтымды болмайды. Сонымен қатар, өлшенген коэффициенттерді анықтау қиын, олардың негізінде барлық критерийтар біріктіріледі.
4	Синтезделген «Парето нүктелері» әдісі және өлшенген сомалар әдісі [49, с.6].	Әдісті қолдану нәтижесі белгілі бір жағдайларда ең ұтымды «Парето нүктесі» болады.	Көп критерийліесепті шешуге субъективті аспект енгізетін сараптамалық бағалау әдісі қолданылады.
5	Мүлдем қолайсыз нұсқаға тыйым салу [50].	Бұл негізгі критерий бойынша нәтижені барынша арттыруға мүмкіндік береді.	Критерийтардың бірі қажетті талаптарға барынша сәйкес келмеген жағдайда ғана қолданылуы мүмкін.
6	Зерттелетін параметрдің идеал мәнінен қашықтығының функциясына негізделген әдіс [50 С. 145-146].	Критерийтардың мәндерін олардың идеалды мәндеріне барынша жақындатуға мүмкіндік береді.	Ұтымды шешу нәтижесінің идеалды нұсқасы белгілі болған кезде ғана қолдануға болады. Критерийтардың нақты мәндерінің олардың идеалды мәндерінен ауытқуы үшін өлшенген коэффициенттерді анықтаудағы қиындықтар.

1.3-кесте жалғасы

1	2	3	4
7	Тізбекті шегінімдер әдісі [51].	Шегінімдердің мәні мен нәтиженің ұтымды нәтижеге жақындық дәрежесі арасындағы байланысты талдауға мүмкіндік береді. Бұл есепті шешуді айтарлықтай жеңілдетеді.	Әр критерийтың маңыздылығын, сондай-ақ, олар үшін жеңілдік деңгейін анықтауда қиындық бар.
8	Жүйелік көп критерийлі ұтымды шешу [52].	Максималды емес, керісінше есепті сәтті шешу ықтималдығын едәуір арттыратын ұтымды мәндерді іздеуге бағытталады.	Бұл әдіс сараптамалық сауалнама арқылы жүзеге асырылады. Бұл көп критерийлі есептерді шешуге субъективті аспектілік сипат береді. Егер сарапшылар ұтымды мәндердің қажетті аймағына сәйкес келетін параметр мәндерін таңдай алмаса, шешім табылмауы да мүмкін.
9	Операцияларды зерттеу әдістері [53].	Әдістердің қарапайымдылығы және барлық мүмкін баламаларды талдау мен салыстырудың салыстырмалы түрде қарапайым модельдері. Әдістер жақсы алгоритмделген. Бұл әдістер үшін жақсы танылған қолданбалы БҚ пакеттері бар.	Салыстыру параметрлері көбейген сайын, әдістер тиімділігін жоғалтады және күрделі тапсырмалар үшін әрдайым қолайлы бола бермейді.

1.3-кесте жалғасы

1	2	3	4
10	Ойын теориясына негізделген әдістер мен модельдер [54].	Ойындар теориясының математикалық аппаратын қолданудың әмбебаптығы.	Көп критерийлі ұтымды шешу есептері үшін жоғары есептеу күрделілігі
11	Анық емес логика әдістері [54, 85 бет, 55].	Анық емес логикаға негізделген басқаруды ұтымды шешу әдістері көбінесе эвристикалық болып табылады.	Меншік функцияларын таңдауда және анық емес енгізу ережелерін қалыптастыруда субъективтілік бар, бұл әсіресе, көп критерийліұтымды шешу есептерін шешудің дәлдігіне әсер етеді.
12	Нейрожелілік [56].	Тәуелсіз айнымалылармен жұмыс істеу мүмкіндігі.	Тек ұтымды шешімдерді табуға мүмкіндік береді. Бұл әдістер әрқашан объектінің параметрлерін ұтымды шешу үшін жоғары дәлдікті қажет ететін тапсырмалар үшін қолданыла бермейді.
13	Интерактивті әдістер [57].	Әдістер жақсы алгоритмделген. Әдістер итерациялар жиынтығынан тұрады, олардың әрқайсысы ШҚТ жасаған талдау және есептеу кезеңдерін қамтиды.	Парето жиынын және/немесе алдыңғы жағын біркелкі жақындату үлкен есептеу шығындарын қажет етеді.Теңдестірілмейтін шешімдер санының артуымен қол жеткізілетін дәлдікке қойылатын талаптардың жоғарылауымен жалғыз шешімді таңдаумен байланысты есептер ұсынылған жиын ШҚТ үшін көп уақытты қажет етеді. Парето фронтының визуализациясында критерийтар саны екіден көп болған жағдайында қиындық бар.

1.3-кесте жалғасы

14	Эволюциялық әдістер [58, 59].	Паретоның бүкіл алдыңғы жағын есептеуге мүмкіндік беретін көптеген шешімдер жасауға мүмкіндік береді.	Төмен жылдамдық пен Парето шешімдердің ұтымдылығына кепілдік берілмейді. Жасалған шешімдердің ешқайсысы шешімдердің басқа нұсқаларына үстемдік етпейтіні белгілі. Әдістер жаңа, дамуды қажет етеді.

Ұтымдылық критерийі бір (немесе бірнеше) [60] ақпараттық (кибернетикалық) қауіпсіздік көрсеткіштері болуы мүмкін – ақпараттың қауіп-қатерлерін іске асырудан келтірілген залалдың шамасы, ақпараттың жайылып кетуінен болған залалды және оны қорғауға жұмсалған шығындарды, ақпаратты қорғауға жұмсалған инвестициялардан түскен пайданы, олардың рентабельділігін және тағы басқаларды қамтитын жалпы шығыстар.

Қойылған есептерді шешу бірқатар себептерге байланысты қиындайды. Ең бастысы, ұтымды шешімді іздеу тұрақсыздық жағдайында жүзеге асырылады, онда қарсыластың іс-әрекетін белгілі бір ықтималдықпен ғана болжауға болады, кейде тіпті мүмкін де болмайды. Қорғау құралдары мен әдістерінің әртүрлілігі, олардың сипаттамалары, қарсылас схемаларының әртүрлілігі, қорғаныс жүйесінің жекелеген элементтерінің осалдықтарын дәл анықтау мүмкін еместігі, біздің елімізде статистикалық мәліметтердің болмауы да қолайлы әдістер тізіміне шектеулер қояды [61].

Жұмыстың басым есебі – АОБ көп тізбекті қорғаныс жүйелерінде және көп бағытты қарсылас жүйелерінде ресурстарды ұтымды бөлудің динамикалық режимінде іздеу, мұнда тараптардың әрқайсысы өз ақпаратын сақтауға және қарсыластың ақпаратын алуға тырысады. Нақты объектілерге «байланыстырылған» жүйелердің кең класы үшін бұл есепті шешу көп контурлы АҚҚ-ның экономикалық және техникалық көрсеткіштерін жақсартуға мүмкіндік береді [62, 63].

Зерттеу объектісі үшін математикалық модельдің құрылысы бірнеше кезеңге бөлінген:

1-кезең) мақсатты функцияны анықтайтын және ұтымды шешуге жататын көрсеткішті таңдау керек. Мұндай көрсеткіштер мыналар болуы мүмкін: жүйенің сенімділігі, ақпараттың тарап кетуінен болатын залал оны қорғауға жұмсалатын шығындар, ақпаратты қорғауға бөлінген ресурстар саны, оларды объектілер арасында бөлу, ақпаратты қорғауға инвестициялардың рентабельділігі және т.б.

2-кезең) мақсатты функция тәуелді болатын жүйенің параметрлері мен сипаттамаларын анықтау керек.

3-кезең) АҚҚ туралы мәліметтерді және қарсы тұрудың ықтимал шарттарын (объектілер бойынша ақпаратты бөлу, объектілер осалдығының қарсы тұру жағдайларына тәуелділігі, жекелеген объектілерге шабуыл жасау

ықтималдығы, объектілерге шабуыл жасау ресурстарының белгілі бір санын бөлу ықтималдығы және т.б.) жинау қажет.

4 кезең) мақсатты функцияның АҚҚ параметрлері мен сипаттамаларына, сондай-ақ қарсыласу жағдайларына, яғни мақсатты функцияның формасына тәуелділік түрін анықтау қажет.

5-кезең) ұтымдылық критерийін таңдаған жөн (ақпараттың тарап кетуінен болған жиынтық залал, объектілер бойынша оның орташа мәні, объектілердің әрқайсысы үшін рұқсат етілген ең жоғары мән және т.б.).

Есептеулерді ұйымдастыру келесі операцияларды қарастырады: есепті шешу әдісін таңдау; компьютерге арналған бағдарламаны құру және жөндеу; есептеулер жүргізу; нәтижелерді неғұрлым ыңғайлы түрде ұсыну; қорытындылар мен ұсыныстарды тұжырымдау.

1.3. Бірінші тарау бойынша қорытындылар және одан әрі зерттеу үшін есептер қою

Қазіргі заманғы АҚҚ – бұл өте күрделі құрылымдар, олар көп тізбекті КҚ жүйелерінің қорғауында болатын көптеген объектілерды қамтуы мүмкін. Аппараттық, бағдарламалық, ұйымдастырушылық құралдар мен қорғаныс әдістерінің әртүрлі конфигурацияларын қамтуы мүмкін мұндай жүйелерді зерттеу қиын есеп болып табылады. Мұндай есептерді, соның ішінде, математикалық модельдеудің әртүрлі әдістерін және АОБ көп контурлы қорғаныс кешендерінің құрамын көп критерийліұтымды шешуды қолдана отырып шешуге болады.

Жоғарыда айтылғандарды ескере отырып, жұмыстың бірінші тарауында келесі негізгі нәтижелер алынды және диссертациялық зерттеудің келесі тарауларында шешуді қажет ететін есептер белгіленді.

1. ISO / IEC TR 13335 сәйкес ақпараттық-коммуникациялық технологиялар сегменті ретінде АКЖ қауіпсіздігін басқару модельдері талданды.

2. ISO/ IEC 27001: 2010 сәйкес «жоспарла – орында – тексер – әрекет ет» моделінің мазмұны ашылды.

3. АОБ АҚ және оның АКЖ басқару құрылымы ақпараттың өмірлік циклі деңгейінде «объект – қауіп – қорғау» тұжырымдамасына және «кибернетикалық кеңістік - коммуникациялық орта - физикалық кеңістік» көп деңгейлі моделіне сәйкес талданды. АҚ АКЖ-ны басқару құрылымы қауіп-қатер модельдеріне сәйкес АКЖ-ны көп деңгейлі қорғау элементтерін барабар таңдауды ғана емес, «жоспарла – орында – тексер - әрекет ет» моделіне сәйкес АР құпиялылығын, тұтастығы мен қол жетімділігін қамтамасыз етуге, сондай-ақ, қорғау тараптарының ресурстарын динамикалық басқару жөніндегі есептерді шешуге мүмкіндік береді.

4. Қолданыстағы АҚҚ ұтымды шешу модельдерін талдау қарастырылған модельдердің көпшілігінің мақсаты АҚ-ға жалпы шығындарды ұтымды шешу екенін көрсетті (Гордон-Леб моделі, К.Задираки моделі). Тек бір ғана модельдер динамикалық режимде АҚ (Глушак-Новиков моделі) объектілері арасында ұтымды қаражат бөлуді іздеуге бағытталған.

Осылайша, диссертацияның бірінші тарауының тұжырымдарына сүйене отырып, әрі қарайғы зерттеулердің есептерін тұжырымдауға болады [62-63].

1. АР көлемі мен құндылығының ұлғаюын, кибершабуылдардың жаппай таралуын, ақпаратты қорғау құралдарының да, шабуыл жасау үшін қолданылатын құралдардың да арсеналын кеңейту мен жетілдіруді ескере отырып, АОБ КҚ ресурстарын динамикалық басқару модельдерін дамытуға бағытталған жаңа зерттеулер қажет. АОБ КҚ ресурстарын динамикалық басқаруды модельдеу кезінде қорғаныс объектілерінің осалдығы функциясын қолданудың келешегі бар. Соңғысы шабуылдың да, қорғаныс ресурстарының да көлеміне байланысты.

2. Тұрақсыздық жағдайында, қарсыластың іс-әрекетін белгілі бір ықтималдықпен ғана болжауға болатын кезде, теориялық және ойын әдістерін қолдану және жағдайдың өзгеру динамикасын ескере отырып, АҚ объектілері арасында шектеулі ресурстарды ұтымды бөлуді іздеу қарсыласу, ақпараттың қауіптерін жүзеге асырудан келтірілген зиянның мөлшерін ең аз шамаға дейін азайтуға мүмкіндік береді.

3. Жұмыстың тақырыбы көп контурлы АКЖ АҚҚ-ға арналған АҚҚ таңдау кезінде көп критериалды ұтымды шешу есебімен тікелей байланысты болғандықтан, АОБ үшін АҚ және КҚ көп контурлы жүйелерінің ұтымды конфигурацияларын іздеу барысында көптеген шешімдерді генерациялау үшін эволюциялық әдістер мен генетикалық алгоритмдерді дамытуға, сондай-ақ бар қауіптердің өзекті болуына байланысты қорғаныс тарабының ресурстарын динамикалық қайта бөлу есебін шешу үшін ГА-ны қолдануға назар аударған жөн.

2 ҚОРҒАУ ОБЪЕКТІЛЕРІ АРАСЫНДА РЕСУРСТАРДЫ БӨЛУДІ ҰТЫМДЫ ШЕШУ

2.1. Теориялық және ойын әдістері негізінде ақпараттық ресурстарға шабуыл жасау және қорғаныс тараптарының қарсылығын модельдеу

Белгісіздік жағдайында тиімді АҚҚ құру үшін маңызды есеп -қорғаныс объектілері арасында ресурстарды бөлудің мүмкін нұсқаларын зерттеу және олардың ішінен ұтымдысын таңдау. Қорғау тарапының мақсаты - қауіп-қатерлердің ықтималдығын азайту. Шабуыл жағы тікелей қарама-қарсы мақсаттарды көздейді. Шабуыл жасаушылар өз ресурстарын киберқауіптерді іске асырудан барынша ұтымдылыққа қол жеткізетіндей етіп бөлуі тиіс. Шын мәнінде, бұл жағдай ойын теориясының есебін қоюға қатысты [64, 65]. Әр тараптың жеңісі қарсыластың стратегиясына байланысты және $o(h,d)$. мақсатты функциямен анықталады

Мұнда жоғарыда тұжырымдалған тұжырымдағы есеп нөлдік сомадағы ойынның асимметриялық жағдайына сәйкес келетіндігін нақтылау қажет. Яғни, бірінші ойыншы ғана жеңе алады (шабуылдаушы (h хакер)). Оның ұтысы залал келтірілген АР құнымен бағаланады. Содан кейін қорғаныс жағының d жоғалуы шабуылдаушының жеңісіне тең.

Мұндай есептерді қою үшін әр тарап (h,d) өзінің жеңіс функциясын біледі деп болжаймыз. Сондай-ақ, әр тараптың өз мақсаттарын іске асыру үшін бірқатар стратегиялары бар.

Жоғарыда айтылғандай, тараптардың әрқайсысының өз есептерін орындау үшін өз ресурстары болады. Тиісінше, шабуылдаушылардың H ресурстары бар. Қорғау жағында D ресурстар бар. Ресурстар саны шектеулі және әртүрлі объектілерға бағытталуы мүмкін.

Шабуылдаушы (шабуылдаушылар) стратегиясы - өз ресурстарын объектілер арасында әртүрлі арақатынаста бөлу:

$$\sum_{k=1}^{l} h_k = H,\ h_k \geq 0, \qquad (2.1)$$

мұнда, k - қорғау объектісінің нөмірі $\left(k = \overline{1,l}\right)$, h_k - объектіде қатерлерді іске асыруға арналған шығындар (ресурстар).

Сол сияқты, қорғаныс жағы ресурстарды бөлудің өзіндік стратегиясын қолданады:

$$\sum_{k=1}^{l} d_k = D,\ d_k \geq 0, \qquad (2.2)$$

мұнда, d_k k-объектіде қорғауды іске асыруға арналған шығындар (ресурстар).

Шабуылдың шығында шабуылдаушы қорғаныс жағына көп зиян келтіруге тырысатындықтан, мақсатты функцияны келесідей беруге болады:

$$o(h_k, d_k) \to \max. \qquad (2.3)$$

Келтірілген залалдың мөлшерін АР немесе ақпараттық инфрақұрылымның құнымен бағалауға болады. Залал мөлшері тараптардың ресурстарын бөлуге байланысты болады.

Қорғаныс жағы қарсы мақсатқа ұмтылады. Қорғау қауіптерді жүзеге асыру нәтижесінде келтірілген зиянның мөлшерін азайту керек. Демек, жалпы жағдайда қорғаныс жағы үшін мақсатты функция келесідей берілуі мүмкін:

$$o(h_k, d_k) \to \min . \qquad (2.4)$$

Теориялық және ойын тәсілін қолдана отырып, келесі кезеңде бағандар қорғаныс ресурстарын бөлу нұсқаларына $\{d_{jk}\}$, ал жолдар шабуыл ресурстарын бөлудің ықтимал нұсқаларына $\{h_{ik}\}$ сәйкес келетін функция $o(h_k, d_k)$ үшін жеңіс матрицасы жасалады. Осылайша, мынаны аламыз:

$$o = \begin{pmatrix} o_{11} & o_{12} & \dots & o_{1n} \\ o_{21} & o_{22} & \dots & o_{2n} \\ \dots & \dots & \dots & \dots \\ o_{m1} & o_{m2} & \dots & o_{mn} \end{pmatrix}, \qquad (2.5)$$

мұнда, o_{ij} – қауіптерді іске асырудан келтірілген зиянның мөлшері. Ойыншылардың таза стратегияларын қолдану мүмкіндігі үшін $\left(i = \overline{(1,m)},\ j = \overline{(1,n)}\right)$

Осы матрицалық ойынның қажетті стратегиясы қорғаныс жағының ресурстарын ұтымды бөлу болып табылады.

Ұтымды стратегияны іздеген кезде қорғаныс жағы *j*-ші бағанды таңдайды деп болжап, шабуыл жағы *i*-ші жолды қарастырады. Бұл жағдайда жеңіс o_{ij} – элемент болады.

Тараптардың мүдделері диаметрлік қарама-қарсы. Ойыншылардың әрқайсысы қарсыластың стратегиясын білмейді. Бұл тараптардың шешім қабылдауын қиындатады.

Егер ойыншылардың әрқайсысы 1 ықтималдығымен белгілі бір стратегияны таңдаса, онда олар таза стратегияны қолданады деп саналады. Бұл жағдайда ойын шешімі таза стратегияларда болады [66]. Ойынның шешімі - әр ойыншының ұтымды стратегиясын анықтау болып табылады. Егер осы стратегияны қолдану басқа ойыншының барлық мүмкін стратегиялары үшін ең үлкен кепілдендірілген жеңісті қамтамасыз етсе, онда ойыншының стратегиясы ұтымды болады [66, 25-б.]. Осыған сүйене отырып, шабуылшы жеңіс матрицасын (2.5) осылай зерттейді. Әрбір *i*-жолда $\left(i = \overline{1,m}\right)$ қорғау стратегиясын таңдауға байланысты o_{ij} ұтыстың ең аз мәні анықталады $\min_j o_{ij}$., яғни шабуылдаушылардың өзінің *i*-таза стратегиясын қолдану нұсқасы үшін қауіпті іске асыру нәтижесінде келтірілген залалдың ең аз мәні анықталады. Ең төменгі ұтыстардың $\min_j o_{ij}$ ішінде біз осы ең төменгі ұтыстың максималды болатын *i*-стратегиясын анықтаймыз. Сондықтан ойынның төменгі бағасын $\alpha = \max_i \min_j o_{ij}$ табу керек . Қорғаныс жағы симметриялы әрекет етеді. Қорғаныс

жағы үшін біз ойынның жоғарғы шекарасын табамыз, ол қауіп-қатер туындаған жағдайда шабуылдаушының ең көп зиян келтіруі мүмкін екенін көрсетеді. Жоғарғы шекара ойындар үшін тараптар қорғауын осылайша табамыз: $\beta = \min_j \max_i o_{ij}$

Егер ойында жоғарғы және төменгі шекаралар сәйкес келсе, онда ойынның ершік нүктесі болады. Яғни $\max_i \min_j o_{ij} = \min_j \max_i o_{ij} = \Psi$ болады. $\psi -$ ойын бағасы. Бұл жағдайда $\max_i \min_j o_{ij}$ шабуылдаушылар және $\min_j \max_i o_{ij}$ қорғаныс жағы үшін ойыншылардың таза стратегиялары ұтымды болады. Шабуылдаушының стратегиясы ұтымды стратегиядан ауытқыған кезде оның пайдасы азаяды. Сол сияқты, қорғаныс жағы өзінің ұтымды стратегиясынан сәл ауытқып, қауіптерді іске асыру нәтижесінде туындауы мүмкін зиянның мөлшері артады.

Егер ершік нүктесі жоқ болса, онда ойынның төменгі және жоғарғы бағаларының табылған мәндері қорғаныс жағының жоғалуы ойынның жоғарғы бағасынан аспайтындығын және кем дегенде ойынның төменгі бағасына тең болатындығын көрсетеді. Ойыншылардың таза стратегиялары ұтымды нәтиже бермейтіндіктен, ойын теориясы аралас стратегияларды қолдануды ұсынады [66, 170-бет].

Шабуылдаушылардың аралас стратегиялары $W_H^0 = (P_1,...,P_m)$ ықтималдықтар жиынтығымен берілген. Ойыншы бастапқы таза стратегияларын қолданады $\{h_i\}\left(i = \overline{1,m}\right)$ және $\sum_{i=1}^{n} P_i = 1,\ P_i \geq 0,\ i = \overline{1,m}.$

Сол сияқты, аралас стратегиялар қорғаныс жақтары өздерінің ықтималдық жиынтығымен берілген: $W_D^0 = (Q_1,...,Q_n) : \sum_{j=1}^{n} Q_j = 1,\ Q_j \geq 0,\ j = \overline{1,n}.$

Сәйкесінше аралас стратегияларды қолдану кезінде қорғаныс жағын жоғалту (шабуылдаушылардың жеңісі) зиянды математикалық күту ретінде анықталады:

$$o^0 = \sum_i \sum_j P_i Q_j o_{ij}. \qquad (2.6)$$

[67, 68] Көрсетілгендей ойынның шешімі сызықтық бағдарламалау есебін шешуге дейін әкеледі.

Ұтымды аралас стратегияның S_D^0 қасиеті бар, оған сәйкес қорғаныс жағының жеңілісі шабуылдушылардың кез келген мінез-құлықтағы ойын бағасының $\psi -$ мәнінен аспайды.

$\psi -$ ойын бағасының мәні алдын-ала белгісіз. Бірінші кезеңде $\psi > 0$ деп санауға болады(бұл үшін o_{ij} барлық элементтердің оң болуы жеткілікті).

Егер қорғаныс жағы аралас стратегияны қолданса және өзінің *i*- таза стратегиясына шабуыл жасаса, онда зиянды математикалық күту келесідей

анықталады: $o_i = o_{i1}Q_1 + o_{i2}Q_2 + ... + o_{in}Q_n$.Ресурстарды бөлу есептерін, оның ішінде қорғаныс жағының ресурстарын динамикалық бөлу есептерін шешкен кезде, ең алдымен, АҚ объектілері арасында ұтымды бөлуді іздеу моделінің мақсат функциясын қалыптастыру қажет.

Осыған байланысты, ресурстар туралы айтқанда, бірінші кезеңде ресурс дегеніміз, ең алдымен, қорғаныс объектілері арасында бөлінуі керек қаржылық ресурстарды білдіреді деп болжауға болады, 2.1-суретті қараңыз. 2.1-суретте қызметкерлер мен клиенттердің дербес деректерін; аумақты, ғимараттар мен үй-жайларды, деректерді беру желілерінің серверлері мен автоматтандырылған жұмыс орындарын; технологияларды (электрондық түрдегі ақпарат, технологиялық процестердің құрылымы); қаржылық қызмет туралы деректерді және т. б. қорғауға жіберу қажет ресурстарды бөлудің (шартты кәсіпорындар үшін) мысалы көрсетілген.

2.1-сурет – Әртүрлі қорғау объектілеріне жұмсалған қаржы ресурстарын бөлу нұсқасының мысалы

Әрине, ресурстарды бөлуді қажет ететін АҚ объектілерінің тізімі өзгеруі мүмкін және компанияның немесе кәсіпорынның бизнес-процестерінің ерекшелігіне байланысты болады. Банк, өндіріс немесе білім беру саласындағы қорғау объектілері әртүрлі, сондықтан ресурстарды (ең алдымен, қаржылық) әмбебап модельді қолдана отырып бөлу қиын.

Сондай-ақ, ресурстарды бөлу туралы айтқанда, қазіргі заманғы қорғаныс жүйелерінің ерекшеліктерін ескеру қажет екенін есте сақтаған жөн. Мысалы,

көптеген компаниялар шабуылдаушылар үшін тұзақтарды қолдана бастады [67]. Бұл технологиялар компаниялардың немесе кәсіпорындардың арнайы, параллель желілеріне негізделген. Бұл желілерде тапсырыс берушінің IT-инфрақұрылымына таралған жасырын желілік тұзақтар мен жемдер орнатылады. Шабуылшылардың ресурстарын мұндай қайта бөлудің барлау немесе тарату сатысында шабуылдарды анықтауға көмектесу ықтималдығы өте жоғары.

Ресурстарды бөлу немесе қайта бөлу туралы айтатын болсақ, біз ұтымды шешу көп критерийлі есеппен айналысамыз. Мұндай есептерді шешу барысында көбінесе арнайы мақсатты функцияларды қолдану қажет. Мұндай функциялар көбінесе сызықты емес және унимодальды емес. Сонымен қатар, мұндай функциялардағы шектеулер сызықты емес және дөңес емес. Мұндай көп критерийлі ұтымды шешу есептеріндегі айнымалылар және АҚ объектілері арасындағы ұтымды үлестіруді іздеу моделінің мақсатты функциялары үздіксіз, тұтас, логикалық, аралас болуы мүмкін.

Көптеген мұндай көп критерийлі ұтымды шешу есептерін шешудің дәстүрлі стратегияларын іске асыру айтарлықтай есептеуді қажет етуі мүмкін. Айта кету керек, табылған шешім өзекті болып табылатын және нәтиже ақпараттық ресурсты жоғалту қаупі тұрғысынан қолайлы болатын уақыт аз болады. Шабуыл жасаушылар шабуыл техникасын үнемі жетілдіріп отырады, сондықтан жағдай үнемі өзгеріп отырады және үнемі жаңа шешімдерді талап етеді.

Мұндай жағдайларда ұтымды шешу есептерін шешудің генетикалық алгоритмдері (ГА) ерекше қызығушылық тудырады.

Алайда, қорғау тарапының ресурстарын динамикалық бөлу есебін шешу үшін ГА-ны әзірлеуге кіріспес бұрын, АҚ объектілері арасында ресурстарды бөлудің мақсатты функциясын қалыптастыру керек.

Белгілі бір ақпараттық жүйенің математикалық моделін жасау кезінде мақсатты функцияға кіретін параметрлердің мәндерін және тәуелділік формасын анықтау қажет [68, 17-б.]. Анықталған кемшіліктерді жою және АҚҚ модельдеу саласындағы соңғы жетістіктерді пайдалану мақсатында АҚ-ның қолданыстағы модельдеріне бірінші тарауда жүргізілген талдау негізінде мақсатты функцияның негізгі компоненттері анықталды. Таңдалған модель үшін мақсатты функция қауіптерді іске асырудан келтірілген залалды білдіреді және түрі осылай болады [64, 110-б.]:

$$o(h_k, d_k) = \sum_{k=1}^{l} o_k(h_k, d_k) = \sum_{k=1}^{l} g_k p_k v_k(h_k, d_k), \qquad (2.7)$$

Мұндағы $k = \overline{1,l}$ – қорғауға арналған объектінің нөмірі;

h_k, d_k – тиісінше, қорғаныс шабуылының ресурстары;

g_k – АҚ k-объектісіндегі АР салыстырмалы мәні;

p_k – АҚ объектісіне шабуыл жасау ықтималдығы;

$v_k(h_k, d_k)$ – АҚ k-объектісінің осалдығы. Осалдық шабуылдаушылар мен қорғаныс жақтарының ресурстарының арақатынасына байланысты.

$o(h,d)$, $o_k(h,d)$, g_k шамалар АР-дің барлық құнына жатады. $v_k(h_k,d_k)$– мән талданатын объектідегі ақпараттың құнына жатады. Қарама-қайшылық белгісіздік жағдайында қарастырылады. Шын мәнінде, киберқақтығыстардың нақты тәжірибесіндегідей, p_k шабуылдың ықтималдығын бағалау мүмкін емес. Сондықтан біз $p_k = 1$, яғни (шабуыл болды) деп санаймыз.

Объектінің $v(h,d)$ осалдығы сәтті шабуылдың ықтималдығы ретінде қарастырылады және шабуылдаушылардың шығындары мен нысанды қорғау шығындарына байланысты.

Бірінші кезеңде мақсатты функцияға кіретін параметрлердің мәні мен тәуелділік формасын табу керек.

Объектілердегі g_k ақпараттың салыстырмалы құндылығын дәл анықтауға болады. Объектілерге p_k шабуыл жасау ықтималдығы мен $v(h,d)$ тәуелділік формаларын анықтау тараптардың тактикасының белгісіздігімен күрделене түсетін маңызды есеп болып табылады.

Тапсырма екі бағыт бойынша орындалды.

1. АҚҚ көрсеткіштерін енгізу: 1) қорғау объектілерінің саны; 2) объектілердегі g_k ақпараттың салыстырмалы құндылығы; 3) оның табиғи қорғалуымен айқындалатын объектінің бастапқы $v(h,0)$ осалдығы; 4) қорғау ресурстарының жалпы саны – $D = \sum_{k=1}^{l} d_k$; 5) қалдық тәуекел.

2. Қарсыластың іс-қимылын бағалау: 1) шабуылдардың сипаты (олардың бағытталуы мен қарқындылығы); 2) объектілерге p_k шабуыл жасау ықтималдығы; 3) шабуыл жасау ресурстарының жалпы саны - $H = \sum_{k=1}^{l} h_k$; 4) шабуыл жасаушылардың $\{h_k\}$ ресурстарын объектілер бойынша ықтимал бөлу.

Мақсатты функция қауіптерді іске асырудан келтірілген залалды ғана емес, сонымен қатар, басқа шамаларды да білдіре алады. Мысалы, қосымша мыналарды ескеруге болады: АОБ-дағы АР-дың жалпы шығындары; АОБ-дағы АҚҚ-ға инвестициялаудан түскен пайда, инвестициялардың рентабельділігі және т. б.

(2.7) функциясы үшін ұтымдылық критерийін қолдану нұсқалары ГА қолдану тұрғысынан мүмкін. Қосымша шарттар енгізілуі мүмкін, атап айтқанда, қорғаныс жағының ресурстарының мөлшеріне немесе $o(h,d)$ бойынша.

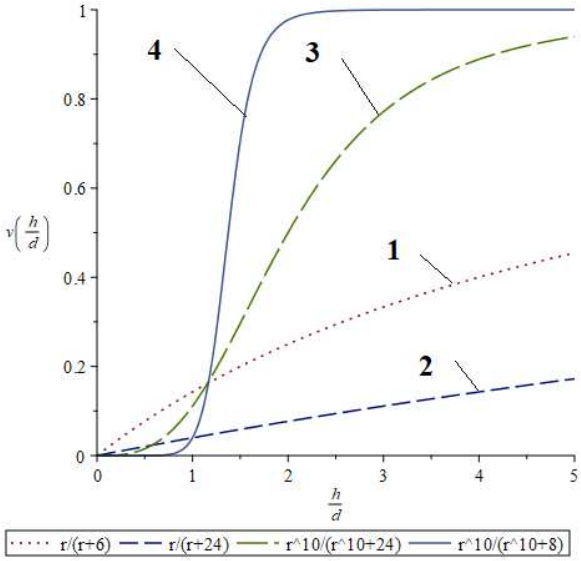
$v(h,d)$ тәуелділіктерді анықтау кезінде келесі ойлар ескерілді. Сәтті шабуылдың ықтималдығы шабуылды жүзеге асыру h шығындарына тікелей пропорционалды және объектіні қорғауға жұмсалатын d шығыстарға кері пропорционалды. Сондықтан *v(h,d)*-ға кіретін *h,d* айнымалылары $r = h/d$. қатынасы ретінде енеді. Жазбаны азайту үшін кейбір жағдайларда біз $d = const$ деп аламыз және *v(h)* тәуелділігін *h* салыстырмалы шама деп қарастырамыз. *v(h,d)*- тәуелділіктері келесі шарттарды қанағаттандыруы керек:

$r=\left(h/d\right)\to 0,$ $v(h,d)\downarrow$ және $r=\left(h/d\right)\to\infty, v(h,d)\uparrow$. Сәйкесінше, біз $y=\left(d/h\right)$ қабылдаймыз. Бұл шарттар түрдің дәрежелік пен көрнекі функцияларын қанағаттандырады [64, 120-б.]:

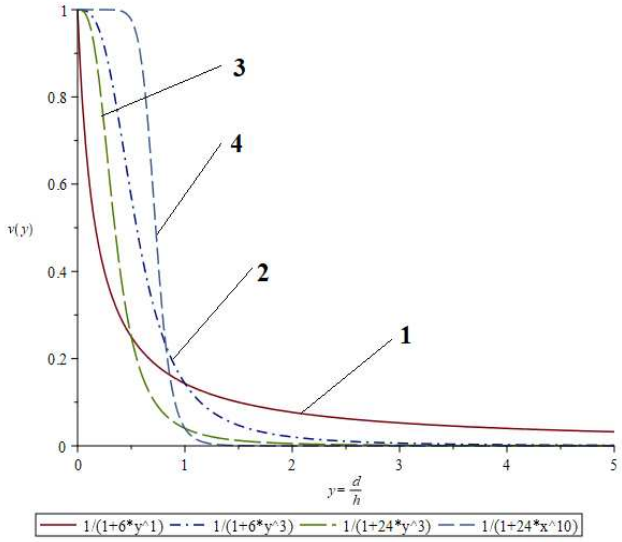
$$v(h,d)=r^n/\left(r^n+a\right) \qquad (2.8)$$

$$v(h,d)=1-e^{-b\cdot r^n}, \qquad (2.9)$$

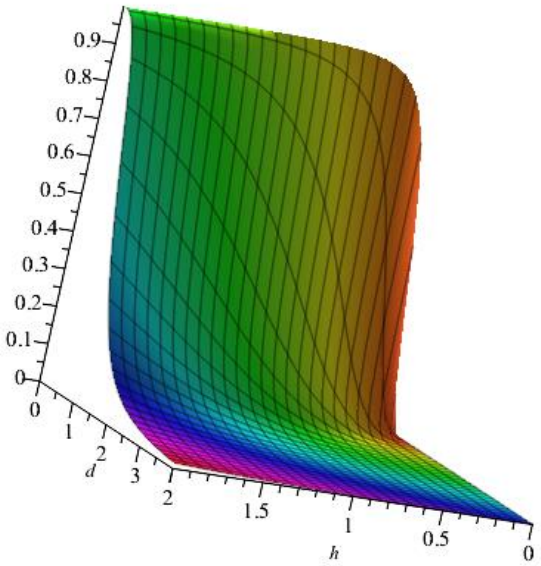
Мұндағы a,b,n - 2.2–2.5-суреттерінде көрсетілген қисықтардың орны мен формасын анықтайтын тұрақтылар.



2.2-сурет – Түрдің дәрежелік функциясы үшін тәуелділіктер (2.8)

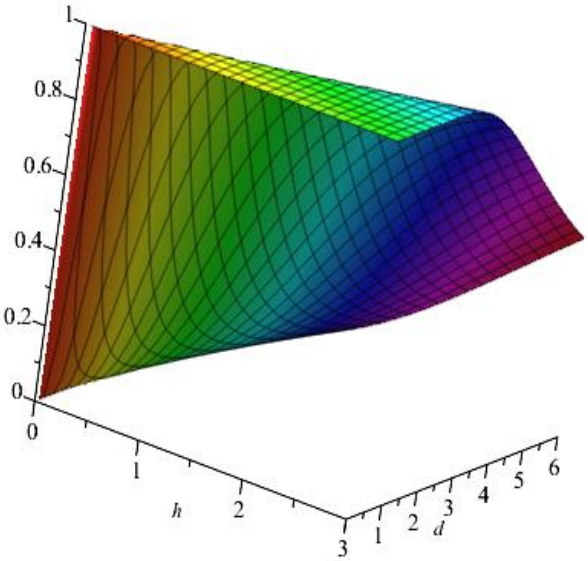


2.3-сурет – Түрдің көрнекі функциясы үшін тәуелділіктер (2.9)



r^3)/(r^3+8)

2.4-сурет – Түрдің дәрежелік функциясының бетіне тәуелділіктер (2.8)



1-exp(-3(r)^2

2.5-сурет – Түрдің көрнекі функциясының бетіне тәуелділік (2.9)

Шешілетін есеп тұрғысынан АОБ үшін АҚҚ шығындарының *a,n* өнімділігі немесе жалпы жағдайда нақты АҚҚ тиімділігінің көрсеткіштері мен оларды сатып алу, қызмет көрсету, жаңғырту шығындарының көрсеткіштері.

Екі тәуелділіктің де формасы ұқсас екенін ескере отырып, олар жоғарыда аталған жағдайларды қанағаттандыратындықтан, болашақта қорғаныс ресурстарын динамикалық бөлу есебін шешудің генетикалық алгоритмін орындау кезінде қарапайым бөлшек- дәрежелік функциялары қолданылды (2.8). *n=1* -де бұл бөлшек-сызықтық тәуелділікті білдіреді. Егер *n>1* болса функция бөлшек-сызықты емес.

n=1-де осалдықтардың бөлшек-сызықтық функциялары АҚҚ-ға жауап береді, олар үшін $\left(h/d < 1\right)$ бастапқы кезеңдерде де инвестиция салу нәтиже береді. Мысалы, периметрді қорғауға, жалған электромагниттік сәулелену және кедергілер (ПЭМИН) арналары арқылы тарап кетуден қорғауға және т.б. байланысты шараларды енгізу АОБ қауіпсіздігінің жалпы дәрежесіне оң әсер етеді.

Бөлшек-сызықты емес *n>1* болса функциялар күрделі техникалық АҚҚ-ның осалдығын сипаттайды. Мысалы, криптографиялық жүйелер. Кілт жоғалған (немесе бұзылған) немесе криптографиялық алгоритмнің осалдығы анықталған сәтке дейін инвестициялар салу нәтиже бермейді, осы сәттен кейін криптожүйенің осалдығы күрт артады. Сол сияқты, вирусқа қарсы қорғанысты және вирусқа қарсы БҚ базаларын жүйесіз жаңарту да жүйенің осалдығының өсуіне әкелуі мүмкін.

n шамасы неғұрлым үлкен болса, кедергі шабуылдарға осал емес шекті мән соғұрлым үлкен болады. Сонымен қатар, қорғаныс жағы мен шабуылдаушылар ресурстарының арақатынасы шекті мәннен асқан кезде өсу аймағы соғұрлым тез артады.

Коэффициентті АОБ-тегі табиғи қауіпсіздік ретінде түсіндіруге болады. Мысалы, типтік ұсыныс - басқа бөлмелермен іргелес есіктері жоқ және баспалдақтар мен шығу есіктерінен алыс орналасқан жеке бөлмелердегі шағын желілердің серверлік бөлмелерін жабдықтау. Сондай-ақ, серверлік бөлмелерге қол жеткізе алатын адамдар тобын шектеу ұсынылады және т.б. Дегенмен, бұл ұсыныстарды бәрі бірдей орындай бермейтінін мойындау керек.

(2.8) және (2.9) мақсат функцияларды қабылдай алатын шектер мен рұқсат етілген мәндерді анықтау үшін шоғырландырылған ақпаратты жинау және талдау талап етіледі. Мұндай ақпараттың көзі - АҚ және КҚ салаларына қатысты есептер. Мысалы, компанияның көлеміне байланысты ақпаратты қорғауға АТ бюджетінің 1%-дан 30%-на дейін кетеді, ал ақпараттың жоғалуы 0-дан 4%-ға дейінгі диапазонда қолайлы деп саналады, бұған қосымша 20%-дан астам ақпараттық активтердің жоғалуы 60%-ға дейін компанияның құлдырауына және банкроттыққа әкеледі [69].

Негізгі есеп қорғаныс тұрғысынан шешім табу болғандықтан, осалдық функциясын (2.8) келесідей ұсынуға болады:

$$v(y) = 1/\left(a \cdot y^n + 1\right) \qquad (2.10)$$

мұндағы $y = d/h$

Тәуелділікті модельдеу нәтижесінде (2.8) және (2.10) сәйкесінше 2.2, 2.4 және 2.3,2.5-суреттерде көрсетілген.

$r \uparrow$-де алынған графиктерден n және a көрсеткіштер бойынша көрінеді және қисықтың пішініне әлсіз әсер етеді. Бұл қисық n және a кез келген түрде болса да бірлікке асимптотикалық жақындайтындығымен байланысты. $0 < r < 1$ -де n шамасы, негізінен, дөңес пішінге, ал a - абсцисса осінен жоғары қисықтың көтерілу биіктігіне әсер етеді.

n және a параметрлердің тәуелділік формасына әсері (2.10) 2.3, 2.5- суреттерінде көрсетілген. n параметрдің әсері негізінен $d < 1$бастапқы аймақта көрінеді. $n \le 1$-де қисықтардың дөңестігі төмен, $n > 1$ -де жоғары бағытталған. a параметр абсцисса осінен жоғары қисықтардың көтерілу биіктігіне әсер етеді. a шаманың өсуімен осалдық азаяды және қисықтар төменге түседі.

Бөлшек-сызықтық функциялар АҚҚ-ға ($d \approx 0$) бастапқы инвестициялар (ұйымдастырушылық, инженерлік-техникалық іс-шаралар мен техникалық АҚҚ-ға) осалдықты монотонды төмендетуге және нұқсанның азаюына әкелетін материалдық жеткізгіштерде сақталатын ақпараттың осалдығын сипаттайды. Әрі қарай d ұлғайған сайын, АҚҚ-ға акша салу тиімділігі төмендейді (бұл пайданың шекті нормасы туралы экономикалық заңға байланысты).

Бөлшек-сызықты емес ($n > 1$, 3, 4-қисықтар, 2.2-сурет) функциялар кедергіні еңсеру үшін айтарлықтай ресурстарды жұмсау қажет болатын компьютерлік жүйелерде айналымдағы ақпараттың қасиеттерін көрсетеді. n көрсеткішінің (2.8) артуы есебінен сызықтық емес өсу кезінде $v(h,d)$-қисық нысан бойынша сатыға жақындайды. Жүйені бұзу үшін айтарлықтай ресурстар қажет болған кезде, мұндай тәуелділік деректерді шифрлауды қолдану кезінде байқалады, содан кейін ақпараттық қауіптерді іске асырудан келтірілген залал күрт артады.

$0 < n < 1$ кезінде (2.8) функция ақпараттың абайсызда болған қауіп-қатердің әсеріне бейімділігін сипаттайды. Кездейсоқ қауіптерге, мысалы, персоналдың қабілетсіздігі, жабдықтың істен шығуы және т.б. мұндай жағдайларда АР иесіне шабуылдаушылар ресурстарды жұмсамай зиян келтірілген.

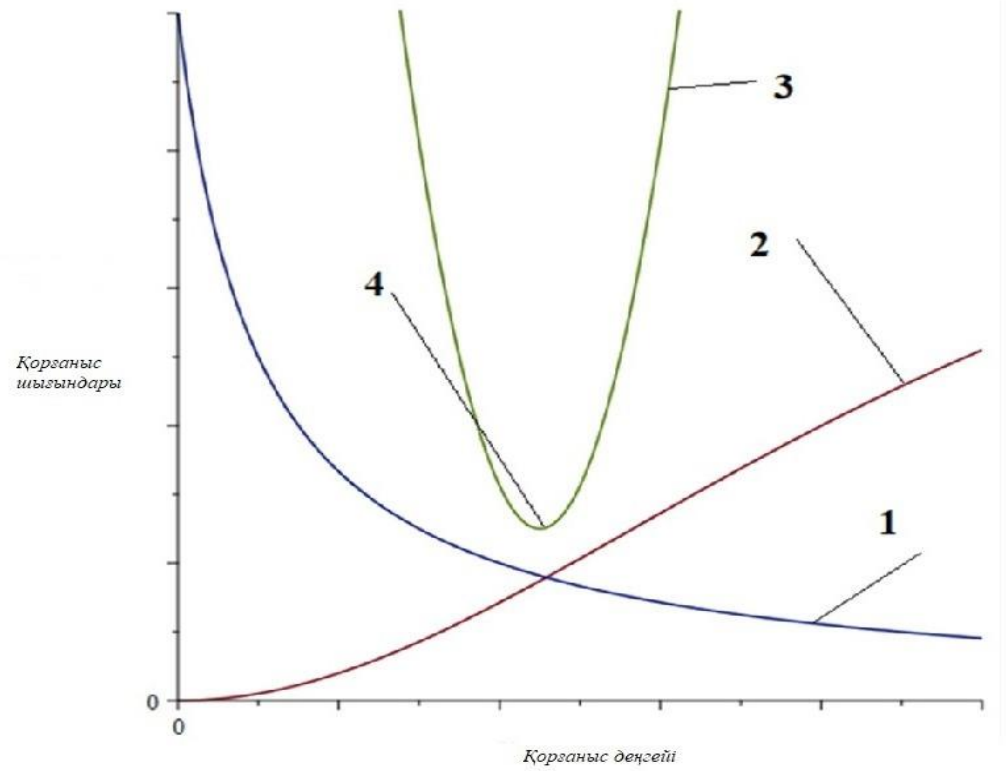
Әр жүйе үшін a,b,n параметрлерді таңдау маңызды есеп болып табылады. a,b,n параметрлердің шамасына техникалық, технологиялық, ұйымдастырушылық, құқықтық, моральдық-этикалық және физикалық АҚ шаралары әсер етеді. Осы шаралардың бір бөлігінің әсері диссертацияның келесі тармағында және келесі тарауларында егжей-тегжейлі қарастырылады. Сәтті шабуыл ықтималдығының шабуыл мен қорғаныс ресурстарының арақатынасына тәуелділік формасын белгілеу есебі өте күрделі және әр нақты жүйе үшін бөлек шешіледі. Тәуелділіктің айқын түрі (2.8) сараптамалық бағалау негізінде немесе статистикалық деректер негізінде белгіленеді.

АҚҚ құру және ақпараттық қауіпсіздік стратегиясы мен саясатын (АҚС) жоспарлау кезінде нақты АҚҚ ерекшеліктерін ескере отырып, мақсатты функцияны ұтымды шешуды орындау маңызды. Қорғау тарапының ресурстарын

жобалау немесе бөлу сатысында бастапқы параметрлерді бағалау кезіндегі қате ақпараттық активтердің айтарлықтай жоғалуына әкеледі.

v(h,d)-алынған мәндер минималды нәтижеге кепілдік бере алмайтындығын ескереміз, өйткені рұқсат етілген мәндердің шекарасы ершік нүктенің болуымен және берілген тепе-теңдік нүктесінен солға немесе оңға ауытқуымен анықталады, 2.1, 2.2 және 2.5-суреттерді қараңыз. Мұндай ауытқу шексіз циклдік процеске әкеледі, онда ешқандай қорғаныс стратегиясы тұрақты нәтижеге кепілдік бермейді. Сондай-ақ, *a* параметрі мақсатты функцияның ұтымды әсеріне айтарлықтай әсер ететіндігін ескеру қажет. Атап айтқанда, АР-ны объектілер бойынша ұтымды бөлу, неғұрлым қорғалған объектілерде АР-дің көп мөлшері болған кезде, D қорғауға арналған ресурстардың бірдей мөлшерімен тиімділігі зор.

2.5-сурет – Ақпаратты қорғауға ресурстарды бөлуді ұтымды шешудің жалпы схемасы



1 - шабуылдардан және АР жоғалудан күтілетін шығындар;
2 - АҚҚ-ға арналған шығындар;
3 - күтілетін жиынтық шығындар;
4 - ұтымды мән

АҚҚ құру кезеңінде ұтымды шешімді іздегенде қарсыластың кез келген іс-әрекеті кезінде біраз уақытқа кепілдендірілген нәтижені қамтамасыз ететін ершік нүктесінің (4) режимі тек белгілі бір құрылымдар үшін және шабуылдаушы тараппен қарсыласудың белгілі бір жағдайларында ғана бар екенін ескеру қажет. Бұл режимді қамтамасыз ету объектілердің осалдығын анықтайтын параметр мәндерін таңдау арқылы жүзеге асырылады. Ресурстардың қажетті санын және

оларды объектілер арасында бөлуді айқындайтын (2.8) және (2.9) мақсат функциялар беттеріндегі жұмыс нүктесін таңдау критерийі мынадай көрсеткіштерді қамтамасыз ету болып табылады, 2.3. және 2.4-суреттерді қараңыз: бір жақты қарама-қайшылық үшін - АР шығындары мен оны қорғауға арналған шығындарды біріктіретін жалпы шығындардың минимумы, екі жақты жағдайда – жалпы пайданың максимумы (АҚҚ-ға инвестициялар салудан түсетін пайданың сомасы және қорғаушы тарап үшін шабуылдаушы тарап туралы ақпарат алудан түсетін пайда немесе симметриялы – АОБ-ға шабуыл жасау құралдарына инвестициялар салудан түсетін пайданың және қорғаныс тарабы үшін шабуыл жасаушы тарап туралы ақпарат алудан түсетін пайда туралы ақпарат). Ұтымды стратегияны іске асырудың сенімділігіне қосымша талаптарды сақтау арқылы қол жеткізіледі: жұмыс нүктесі көрсетілген шарттар орындалатын аралықтың шекарасынан біршама қашықтықта болуы, сонымен қатар жұмыс нүктесінің маңында объектілердегі ресурстардың ұтымды арақатынасында айтарлықтай өзгерістер болмауы керек. Осы жағдайларды қамтамасыз ету қажетті ресурстарды анықтауға мүмкіндік береді, сайып келгенде бұл АОБ үшін ұтымды АҚҚ құруға жол ашады.

2.2. Кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді ұтымды шешу есебін шешуге арналған генетикалық алгоритм

Диссертацияның бірінші тарауында жүргізілген талдау нәтижесінде генетикалық алгоритмдердің (ГА) ресурс мөлшеріне қойылған таңдау мен шектеулердің көп критерийлігі жағдайында ресурстарды бөлуді ұтымды шешу есептеріндегі артықшылықтары атап өтілді. Мұндай артықшылықтарына мыналарды жатқызуға болады:

1. ГА дәстүрлі әдістердегідей нүктеден нүктеге ауысудың орнына бір уақытта бірнеше іздеу кеңістігін пайдаланады. Бұл классикалық ұтымды шешу әдістерінің кемшіліктерінің бірін – мақсатты функцияның жергілікті экстремумына түсу қаупін жеңуге мүмкіндік береді.

2. ГА жұмыс барысында ешқандай қосымша ақпаратты пайдаланбайды. Бұл оның жұмыс жылдамдығын едәуір арттырады. Еркін нүктеде параметрлердің және мақсатты функцияның рұқсат етілген мәндерінің жиынтығы басты ерекшелігі балады.

3. ГА жаңа шешімдерді құру үшін ықтималды ережелерді де, бір шешімнен екіншісіне ауысу үшін детерминделген ережелерді де қолданады. Кездейсоқтық пен детерминизм элементтерін бір уақытта қолдану оларды бөлек қолдануға қарағанда едәуір үлкен әсер етеді.

Жоғарыда айтылғандарды ескере отырып, диссертациялық жұмыстың осы бөлімінде АҚҚ шығындарының экономикалық орындылығының көрсеткіштерін анықтау және объектілер арасында қорғаныс жағының ресурстарын динамикалық қайта бөлу қажет болған жағдайда ұтымды шешімді іздеу үшін ГА синтезі есепсі шешіледі.

Генетикалық алгоритмнің жұмыс принципі табиғи эволюция мен популяциялық генетика механизмдерін модельдеуге негізделген [70]. Графикалық түрде ГА жұмысының схемасы 2.6-суретте көрсетілген.

Диссертациялық жұмыстың осы бөліміндегі *a,n* параметрлерді анықтау үшін ГА-ны АОБ кибернетикалық қауіпсіздігін қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді ұтымды шешу есебін шешу үшін пайдалану ұсынылады. Ресурстарды бөлу көбінесе бұрын көрсетілгендей ақпараттық ресурстардың осалдығының мақсат функциясының түріне әсер ететін *a,b,n,* шамаларды айқындайды (2.10).

ГА келесі терминологиямен жұмыс істейді [70, 16-б.]:

Хромосома – тұқым қуалайтын ақпараттың тасымалдаушысы. Хромосомалардың жиынтығы (әр хромосома үшін мақсатты функцияның (МФ) немесе МФ параметрінің мәні бар) жеке дарақты сипаттайды. Хромосома гендерден тұрады.

Гендер – тұқым қуалайтын ақпаратты кодтау элементтері. Ақпаратты биттік кодтау гендер ретінде пайдаланылуы мүмкін (яғни, биттердің көмегімен МФ сипаттауға болады).

Дарақ(Особь) – хромосомалардың жинағы. Дарақ – бұл ГА қолдану кезінде МФ мәнін іздейтін параметрлер жиынтығы.

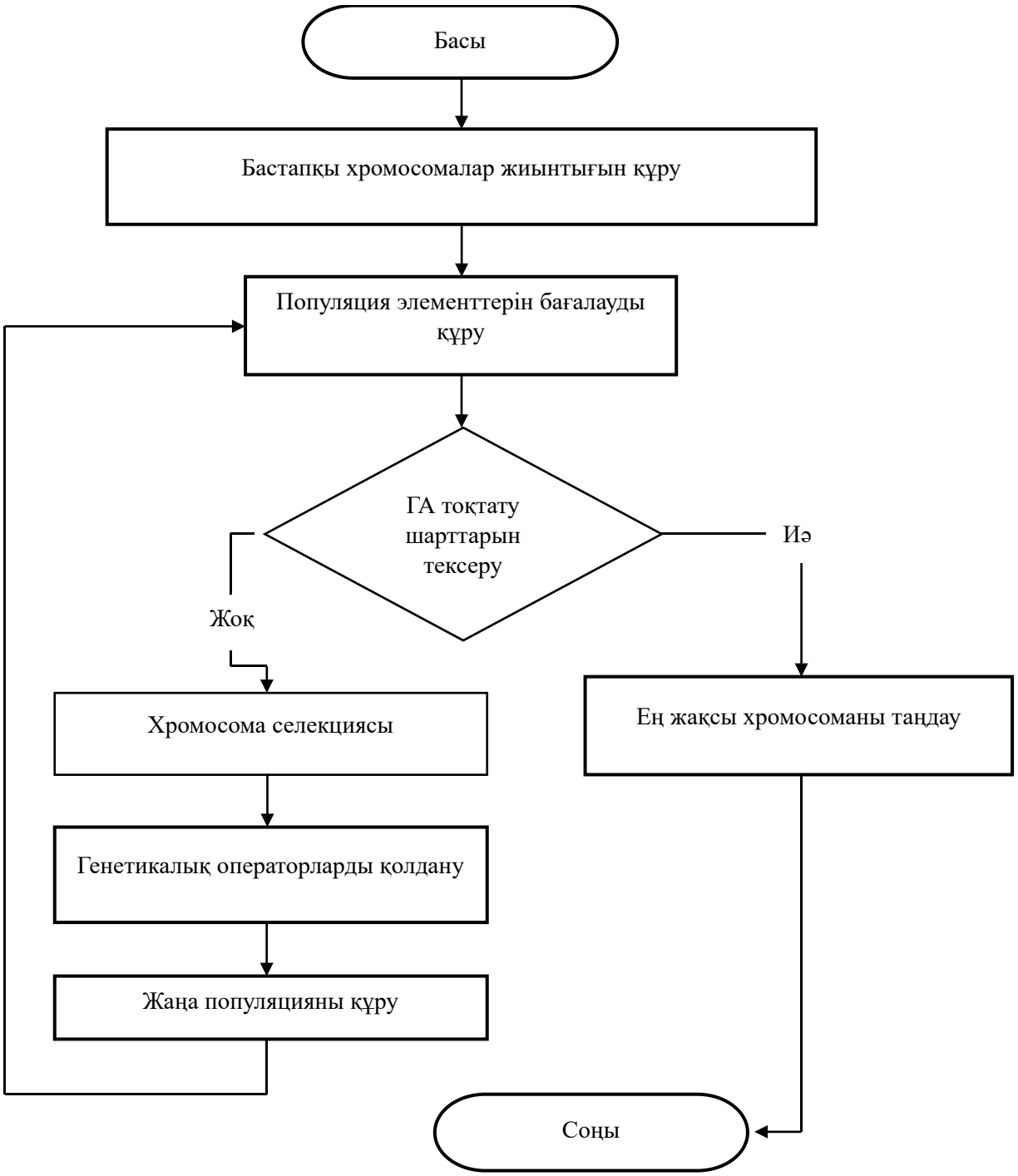
Дарақтың жарамдылығы – бұл МФ-тің қажетті мәніне қатысты осы параметрлер жиынтығы үшін МФ мәні.

ГА әрекеті [70, 22-б.]:

Хромосомалардың бастапқы популяциясының генерациясы – кездейсоқ таңдалған МФ мәндері.

Селекция – көбею үшін ең жақсы бейімділігі бар дарақтарды таңдау. Таңдауды МФ мәні бойынша сұрыптау деп түсіндіруге болады. Жеке дарақтардың икемделу мәні неғұрлым жоғары болса, олардың ата-аналық гендердің келесі ұрпақтарында шағылыстыру және мұрагерлік мүмкіндігі соғұрлым жоғары болады.

Кроссовер (немесе кроссинговер) - шағылыстыру. Кездейсоқ түрде ата-аналардың хромосомаларының биттері арасындағы үзілу нүктесі таңдалады. Үзілу нүктелері – жолдағы іргелес биттер арасындағы бөліктер. Ата-аналық құрылымдар белгілі бір уақытта екі сегментке бөлінеді. Әртүрлі ата-аналар дарақтарының тиісті сегменттері бір-біріне жапсырылады. Жапсырылғаннан кейін ұрпақтардың екі генотипі алынады.



2.6-сурет – ГА жұмысының жалпы сызбасы

Жоғарыда айтылғандай, АОБ үшін АҚҚ шығындарының өнімділігін сипаттайтын *a,n* параметрлер функционалды *v(h,d)*-тәуелділіктің түріне айтарлықтай әсер етеді.

2.1-кестеде АОБ үшін АР осалдық дәрежесіне әсер ететін *a* параметрін зерттеу мысалында көрсетілген есепті шешудің бастапқы деректері көрсетілген.

2.1-кесте – Есепті шешудің бастапқы параметрлері

АОБ-да ақпаратты қорғауды қамтамасыз ету жөніндегі жұмыстардың ірілендірілген тізбесі (а –ның ең жоғары мәнін айқындау үшін) Укрупненный перечень работ по обеспечению		
№	Жұмыстар тізімі	Белгіленуі
1	Кешенді АҚҚ жобалау, әзірлеу және орналастыру	***A***
2	АҚ (АҚҚЖ) қамтамасыз ету жүйесін жетілдіру	***B***
3	АҚ қақтығыстарын анықтау, қақтығыстарға ден қою, АОБ үшін тәуекелдерді болжау	***C***
4	АҚ жеке объектілері арасындағы байланыстарды азайту және қысқы қаттылық компоненттерін біріктіру	***D***
5	АОБ бизнес процестерінің ерекшелігіне сәйкес келетін АҚ ұйымдастыру шараларын әзірлеу	***E***
Бөлінетін ресурстарды шығыстар баптары бойынша топтастыру (Ресурстарды АҚ және КҚ инвестициялау түрлері)		
1	АҚ-ға арналған материалдық және қаржылық шығындар	МҚШ
2	АҚ және АОБ КҚ қамтамасыз ету бойынша жобаларға тартылған адам ресурстары	АР
3	АҚ және АОБ КҚ саласындағы жобаларды басқаруға арналған шығындар	БШ
4	АҚ және АОБ КҚ қамтамасыз етуге арналған басқа да шығындар	ӨШ
АҚО үшін АҚ және КҚ бойынша іс-шараларды енгізуден бәсекелестік артықшылықтар (Ұтымдылық критерийлері)		
1	Бәсекеге қабілеттілік деңгейін арттыру және жаңа нарықтар	БҚ
2	Инновацияларды дамыту және бизнес процестерге цифрлық технологияларды енгізу	ИД
3	АТ шығындарын азайту	ША

a,n параметрлерді анықтау процесінде оптималдылық критерийлерін келесідей сипаттауға болады:

$$F_k = \sum_i \sum_j I_j \cdot E_{ijk} \cdot X_{ijk} \tilde{\to} \max, \qquad (2.11)$$

мұнда $k = 1,2,3$ 2.1-кестеде оптималдылық критерийлері үшін ($k = 1$ (БҚ үшін), $k = 2$ (ИД), $k = 3$ (ША);

$I_j -$ КҚ және АҚ қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлудің таңдап алынған ұтымды нұсқасындағы басымдық (маңыздылық) (2.1-кестені қараңыз.), $\sum I_j = 1$;

$i = 1(A),2(B),3(C),4(D),5(E) -$ жұмыс түрлері жұмыс тізбесінен көрініс (1-кестені қараңыз, АОБ ерекшеліктеріне байланысты өзгеруі мүмкін);

$j=1$ МҚШ үшін, $j=2$ АР үшін, $j=3$ БШ үшін, $j=4$ ӨШ үшін (2.1-кесте) – АОБ-ға АҚ мен КҚ-ны қамтамасыз ететін қаражат пен шараларға инвестициялық салымдардың (ресурстардың) түрлері;

АОБ-ға АҚ мен КҚ-ны қамтамасыз ететін қаражат пен шараларға инвестициялық салымдардың (ресурстардың) түрлері;

X_{ijk} – айнымалы, егер 2.1-кестедегі тізбедегі i жұмыс j инвестициялық салымды іске асыру үшін пайдаланылса, 1-ге тең . Болмаса, 0-ді қабылдаймыз;

$E_{ijk} - k$ ұтымдылық критерийты қамтамасыз ететін j инвестициялық салымды іске асыру үшін орындалатын 2.1-кестедегі тізбедегі i жұмыс түрлерінің тиімділігі ;

$\tilde{\to}$ – a,n параметрлердің ұтымды мәніне қол жеткізу.

АҚ және КҚ саласындағы жобаларды іске асыруға компанияда (кәсіпорында) бар бөлінетін ресурстарға шектеулерді былайша беруге болады:

$$Q = \sum_i \sum_j I_j \cdot l_{ijk} \cdot X_{ijk} \le A_j, \qquad (2.12)$$

мұнда l_{ijk} – k ұтымдылық критерийты қамтамасыз ететін i түріндегі жұмыстарды орындаумен байланысты j ресурстардың шығындары (немесе еңбек сыйымдылығы) ; A_j – k ұтымдылық критерийты қамтамасыз ететін i түріндегі жұмыстарды орындаумен байланысты j ресурстарды инвестициялау бойынша шектеу .

Есепті шешудің құрылымын анықтайтын шектеулер (немесе шешім матрицаларындағы 0 және 1 мәндерін қою) төменде сипатталған.

Шектеу (2.13) k -ұтымдылық критерийі үшін АОБ-да АҚ мен КҚ қамтамасыз ететін j ресурстар бағыты бойынша 2.1-кестедегі тізбеге сәйкес i жұмыстардың ең болмағанда біреуі пайдаланылатынын білдіреді:

$$\sum_i X_{ijk} \ge 1. \qquad (2.13)$$

Шектеу (2.14) k ұтымдылық критерийі үшін i түрдің жұмысы кезінде j ресурстар кем дегенде бір рет пайдаланылатынын білдіреді:

$$\sum_j X_{ijk} \ge 1. \qquad (2.14)$$

Шектеу (2.15) j ресурстарды бөлудің кез келген бағыты бойынша i түріндегі жұмыстардың кез келген бағытта k ұтымдылықтың ең болмағанда бір критерийін қалыптастыруға қатысуы тиіс дегенді білдіреді:

$$\sum_k X_{ijk} \ge 1. \qquad (2.15)$$

Есептің осы тұжырымында ұтымды шешім табу проблемалары келесідей:

1) есеп көп критерийлі;

2) (2.13)–(2.15) шектеулердің түріне байланысты ұтымды шешімдерді іздеудің белгілі әдістері тиімсіз болады немесе көптеген есептеу ресурстарын қажет етеді. Мысалы, қорғаныс объектілері үшін АҚ және КҚ құралдарының ұтымды құрамын іздеу есептерінде кеңінен қолданылатын бұтақтар мен шекаралар әдісі [71] (дискретті бағдарламалаудың комбинаторлық әдісі) үкімді ішкі жиындарға (тармақтау деп аталатын) рұқсат етілген шешімдер жиынтығын дәйекті түрде бөлуге дейін азайтады. Ішкі жиындар үшін сәйкесінше бағалар (шекаралар) есептеледі. Бұл, сайып келгенде, есептің шешімін анық қамтымайтын ішкі жиындарды жоюға мүмкіндік береді. Алайда, (2.13) - (2.15) шектеулерде теңсіздік белгілері бар. Сондықтан тармақталу ережелерін нақтылау және ішкі жиындардың шекараларын есептеу қиын немесе мүмкін емес. Мұндай пайымдауды осы көп критерийлі есепті шешудің басқа әдістеріне сәйкес келтіруге болады. Жоғарыда айтылғандарды ескере отырып, есептің шешімін іздеу алгоритмі ретінде (2.11)–(2.15) генетикалық алгоритмді қолдану ұсынылды, 2.7-суретті қараңыз.

Беллман–Заде принципіне негізделген шешімнің тартымдылығын есептей отырып, ГА жалпыланған схемасы 2.7-суретте көрсетілген.

Жұмыстың басымдылығы сараптамалық жолмен, мысалы, АОБ АҚ жағдайының аудиті негізінде көрсетілуі мүмкін. Немесе алгоритмнің жұмыс қабілеттілігін тексеру үшін. Мысалы, 2.2-кестедегідей.

2.2-кесте – АОБ-да жұмыстар жүргізудің басымдылығын бөлу мысалы

№	*Ресурстарды АҚ және КҚ инвестициялау түрлер*	*Басымдық (B(2) үшін АҚОЖ-ны жетілдіру)*
1	АҚ-ға арналған материалдық және қаржылық шығындар (МҚШ)	0,29
2	АОБ АҚ және КҚ (РА) қамтамасыз ету жөніндегі жобаларға тартылған адами ресурстар	0,28
3	АОБ АҚ және КҚ (БШ) саласындағы жобаларды басқаруға арналған шығындар	0,23
4	АОБ АҚ және КҚ (ӨШ) қамтамасыз етуге арналған басқа да шығындар	0,2

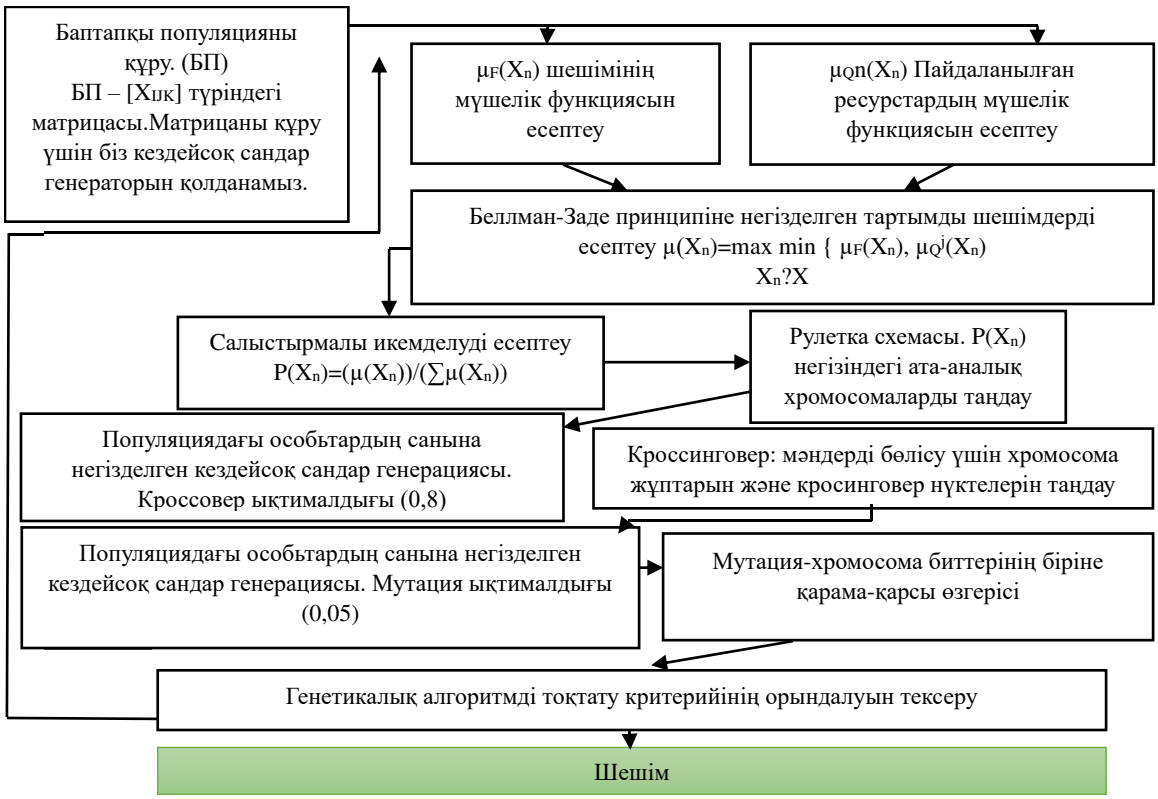
Біздің есебіміз үшін, жалпы жағдайда, модель түрдің үш $X^*_{ij1}, X^*_{ij2}, X^*_{ij3}$ ұтымды шешімін табуды қамтиды (ұтымдылық критерийтардың санына сәйкес):

$$\left\| X^*_{ijk} \right\| = \begin{bmatrix} x^*_{11k} & x^*_{12k} & \dots & x^*_{1jk} \\ x^*_{21k} & x^*_{22k} & \dots & x^*_{2jk} \\ \dots & \dots & \dots & \dots \\ x^*_{i1k} & x^*_{i2k} & \dots & x^*_{ijk} \end{bmatrix}, \qquad (2.16)$$

Мұнда k ұтымдылық критерийінің нөмірі; $x_{ijk}^{*} = 0 \vee 1 -$ дарақ генінің мүмкін күйі.

АОБ АҚ және КҚ қамтамасыз ету саласында қалыптасқан нақты тәсілдерді ескере отырып, кәсіпорын немесе компания 2.1-кестеде келтірілген барлық критерийтарды ескере отырып, бір уақытта тек бір ғана жұмыс түрін жүргізе алады деп қабылдаймыз. Бұл барлық жұмыстарды дереу жүргізу барлық қорғаныс объектілері үшін ақпаратты қорғау контурларының жұмысын бірден бұзатындығымен түсіндіріледі, сондықтан қысқа уақытқа болса да, барлық қорғауды әлсіретеді немесе жояды.

2.7-сурет – Беллман–Заде принципіне негізделген шешімнің тартымдылығын есептей отырып, ГА-ның жалпыланған схемасы



Сондықтан біз тек $i \in [1;5],\ j \in [1;4].$ екі индекс қатысатын X_{ij}^{*}ұтымды шешімді табу есебін шешуге көшеміз.

Әр шешім түрдің екілік матрицасын білдіреді:

$$\left\| X_n \right\| = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \\ x_{51} & x_{52} & x_{53} & x_{54} \end{bmatrix}, \tag{2.17}$$

мұнда n дегеніміз Х- хромосоманың нөмірі және $x_{ij} = 0 \vee 1.$. ГА қолдану үшін x_{ij} мәндерді екілік реттілік форматында кодтау керек. Шешімді немесе екілік

матрицаны ұзындығы 20 биттік тізбектен тұратын хромосома ретінде елестетуге болады (5*4 өлшемді матрица).

Суретте мұндай жазбаны қабылдауды ыңғайлы ету үшін жеке топтарды 4 биттен бөлетін бос орындар қолданылады.

Бірінші популяция кездейсоқ сандар генераторының көмегімен жасалады. Бірінші кезеңде алты хромосома қаралды, 2.8-суретті қараңыз. 2.8-суретте көрсетілген әр реттілік ГА үшін бастапқы популяцияны құрайтын алты хромосоманың бірі болады.

X_1=	1011	0011	1101	0001	1011
X_2=	0100	0110	1101	0101	0000
X_3=	1000	0000	1010	1101	0000
X_4=	0111	0011	0111	0001	1010
X_5=	0101	1010	0010	0110	1001
X_6=	1111	0011	1000	0101	1011

2.8-сурет – ГА үшін бастапқы популяция схемасы

ГА іске асыру барысында қолайлы шешімдерді таңдауда ұтымды шешу есебін қою үшін әрбір мұндай шешімнің жарамдылығын бағалау қажет. Бөлінген ресурстарға шектеулер, сондай-ақ, ұтымды нәтижелерге қол жеткізу анық емес деп санаймыз. Компаниялардың ресурстарды ұтымды шешу іс-тәжірибесінде қорғаныс жағы – бұл жағдай [72] жұмыста егжей-тегжейлі сипатталған . Яғни, біз анық емес математикалық бағдарламалау есепсімен айналысамыз. Жоғарыда айтылғандардың негізінде Беллман–Заде принципін қолдана отырып, шешімнің тартымдылығын анықтау ұсынылады [73]. Математикалық тұрғыдан, бұрын қабылданған белгілерді ескере отырып, бұл принципті келесідей жазуға болады:

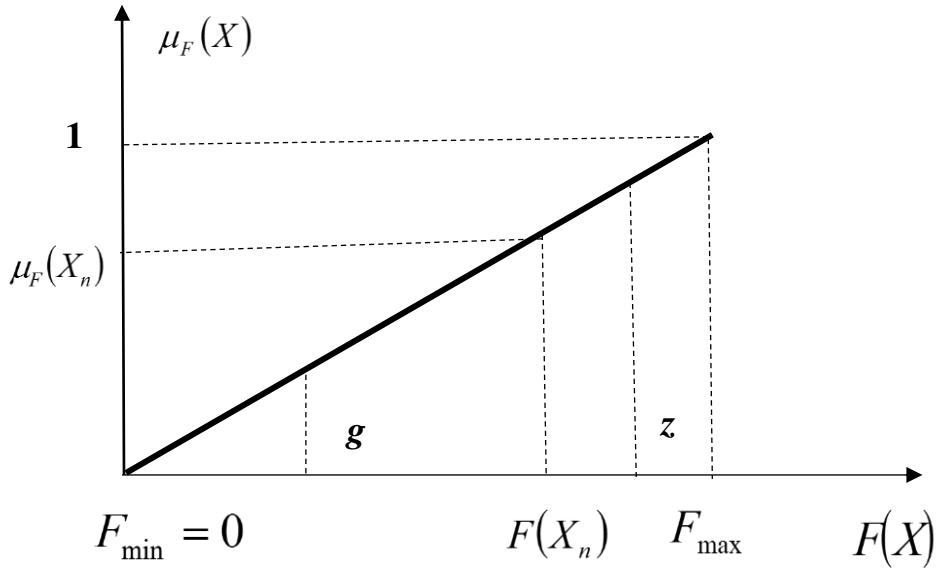
$$\mu(X_n) = \max_{X_n \subset X} \min \left\{ \mu_F(X_n), \mu_Q^j(X_n) \right\} \tag{2.18}$$

Модельдеу барысында алынған шешімдерді немесе яғни F_k критерийінің экстремалды мәнге жету дәрежесін бағалауға болады:

$$\mu(X_n)=\begin{cases}0,\ for\ F(X_n)\le z-g;\\ \mu(X_n,g)\ for\ z-g<F(X_n)<z;\\ 1\ for\ F(X_n)\ge z,\end{cases} \tag{2.19}$$

Мұнда $x\in[g,z]$, $g,z-$ жиынның шекаралары, 2.9-суретті қараңыз.

$F_{\max},F_{\min}-$ тиісінше, 2.1-кестеде ұтымдылықтың үш критерийі үшін мүмкін болатын ең жоғары және ең төменгі мәндер (*k=1* (БҚ үшін), *k=2* (ИД), *k=3* (ША). ГА көмегімен есептерді шешу барысы бойынша $F_{\max},F_{\min}-$мәндер қорғау тарабының ресурстары шектелмеген деген болжам негізінде айқындалады және ол тиісінше 2.1-кестеде қамтылған жобалар бойынша барлық жұмыстарды іске асыра алады. Қарама-қарсы жол беру - қорғау жағында жобаларды жүзеге асыру үшін ресурстар жоқ. Шабуылдаушы тарап үшін, қажет болған жағдайда, алдыңғы бөлімде сипатталған теориялық және ойын модельдерінің аппаратын қолдана отырып, пайымдауды осылай жасауға болады.



2.9-сурет – Шешім сапасын анықтау процесінде тиістілік функциясын алудың жалпы схемасы

Барлық $F_{\min}$ мәні үш *k* –үшін де бастапқыда нөлге тең. $F_{\max}$ мәнін (2.11) формуланы қолдану арқылы табуға болады .

k ұтымдылық критериін қамтамасыз ететін *j* инвестициялық салымды іске асыру үшін орындалатын 2.1-кестедегі тізімдегі *i* жұмыс түрінің тиімділігі үшін $E_{ijk}-$ мәндерді сараптамалық сауалнама негізінде анықтаймыз. $X_{ijk}-$бірлік матрицасы. Бұл жағдайда $x_{ijk}=1.$ Мысалы, деректерді өңдеу кезінде ресурстарды бөлу есебін шешу барысында келесі кесте алынды, 2.3-кестені қараңыз. Жұптық салыстырулардың матрицасы Т.Саатидің иерархиялық әдісін [74] және арнайы БҚ немесе Excel-де қолдану негізінде құрылады, 2.10-суретті қараңыз.

k_1 ұтымдылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	АР	БШ	ӨШ
A	25	3	5	3
B	72	4	6	5
C	23	2	7	2
D	52	6	1	7
E	26	4	5	6
k_2 ұтымдылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	РА	БШ	ӨШ
A	45	6	7	7
B	32	2	5	1
C	55	2	1	2
D	71	6	3	3
E	25	4	4	3
k_3 ұтымдылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	РА	БШ	ӨШ
A	76	4	5	4
B	22	2	5	2
C	51	2	1	2
D	58	6	1	7
E	27	4	4	5

Кесте 2.3 - ұтымдылық критерийлері және АОБ АҚ және КҚ ресурстарына инвестициялау түрі үшін жұптық салыстыру матрицалары

Есептеулер нәтижесінде біз мынадай мәндерді аламыз $F_{\max 1}=72{,}86$, $F_{\max 2}=79{,}56$, $F_{\max 3}=80{,}54$.

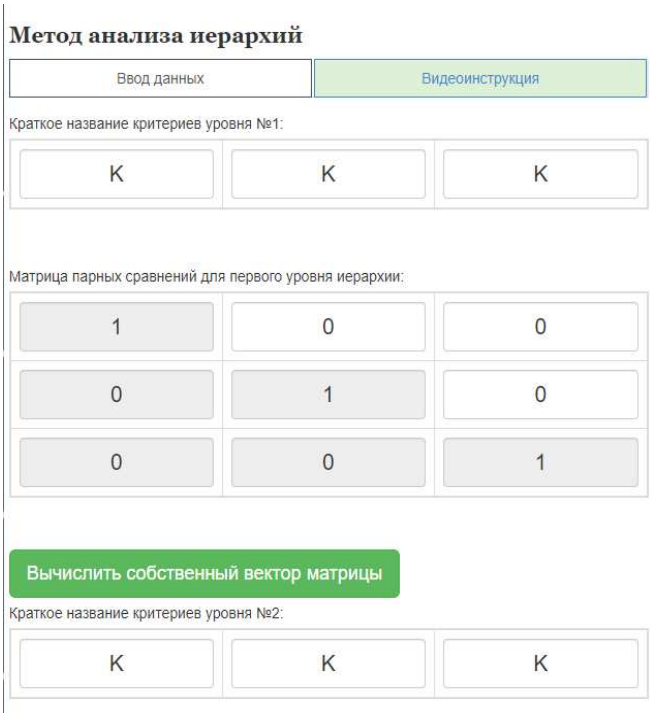
Осылайша, алынған шешімнің сапасына қатысты функцияны толық анықтауға болады – $\mu_F(X_n)$.

Әр шешімнің жарамдылығын өрнек негізінде бағалаймыз (2.8). Түр ресурстарына шектеуді орындау дәрежесі (2.2) жалпы жағдайда келесі тиістілік функциясымен сипатталады:

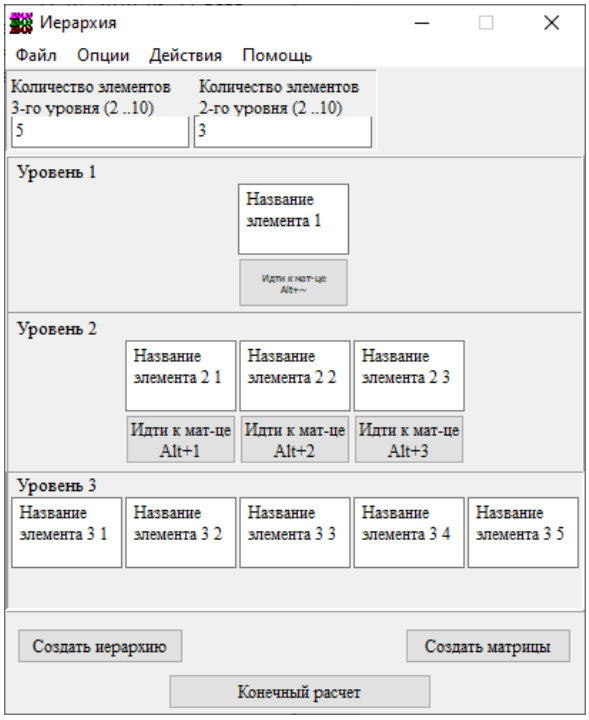
$$\mu_Q^j(X)=\begin{cases}0,\ for\ Q^j(X_n)\geq Q^{j*};\\ \left(Q^{j*}-Q^j(X_n)\right)/\left(Q^{j*}-A^j\right)\ for\ A^j<Q^j(X_n)<Q^{j*};\\ 1\ for\ Q^j(X_n)\geq A^j,\end{cases} \qquad (2.20)$$

Q^{j*} – (2.20) өрнектің сол жақ бөлігі үшін барынша рұқсат етілген мәндер;

$Q^j(X_n)$ – (2.20) хромосома үшін есептелген өрнектегі сол жақ бөліктің мәні.



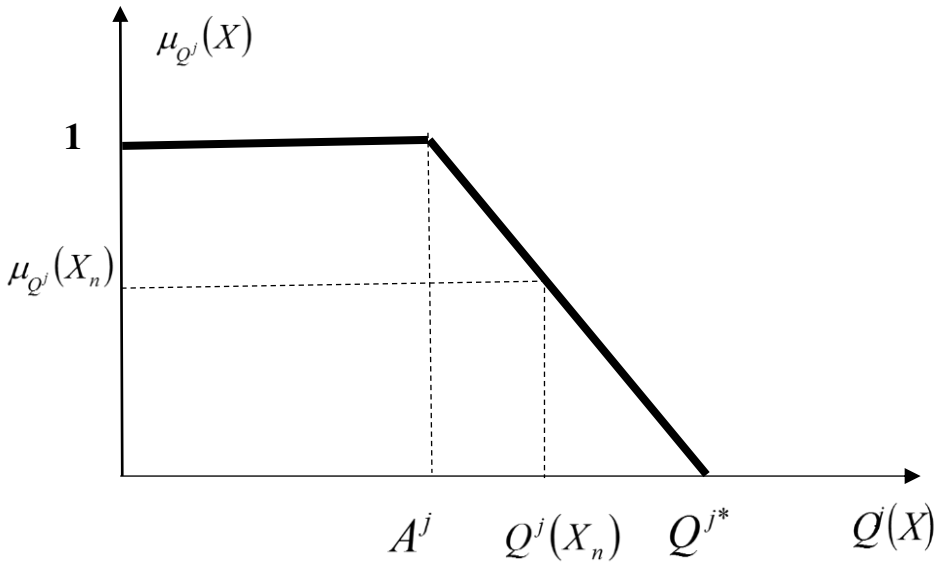
а) - Онлайн сервистің көмегімен Т. Саатидің иерархиялық әдісін қолдану негізінде жұптық салыстыру матрицаларын құру мысалы



б) - Сериялық БҚ қолдана отырып, Т. Саатидің иерархиялық әдісін қолдану негізінде жұптасқан салыстыру матрицаларын құру мысалы

2.10-сурет – Т. Саатидің иерархиялық әдісін қолдану негізінде жұптасқан салыстыру матрицаларын құру мысалдары

Графикалық түрде, өрнекке (2.19) сәйкес тиесілік функциясын осылай көрсетуге болады, 2.11-суретті қараңыз.



2.11-сурет – АОБ АҚ және КҚ қамтамасыз ету үшін пайдаланылатын ресурстардың тиістілік функциясының жалпы схемасы

Бұрын көрсетілгендей, АҚ және КҚ бойынша жобаларға жұмсалған ресурстар мөлшеріне шектеу сараптамалық бағалауды қолдану нәтижесінде белгіленген.

Мысалы, жұмыстың осы параграфының шеңберінде өлшемсіз көріністе ресурстарға (ұлттық валюталарға байланыстырмай шартты ақша бірліктерінде) мұндай шектеулер қойылды. Бірінші ресурс үшін (АҚ – МҚШ-ға арналған материалдық және қаржылық шығындар, тиісінше $A^j = 40,\ Q^{j^*} = 50.$. Қалған ресурстар - РА, БШ, ӨШ үшін тиісінше $A^j = 2, Q^{j^*} = 3.$ $Q^j(X_n)$ функция мына формула бойынша есептеледі:

$$Q^j(X_n) = \sum l_{ijk} \cdot x_{ijk}, \tag{2.21}$$

мұнда l_{ijk} – k-ұтымдылық критерийін қамтамасыз ететін i- түрдегі жұмыстарды орындаумен байланысты j ресурстардың шығындары (немесе еңбек сыйымдылығы).

А-Е жұмыс түрлерінің ұсынылған жіктемесіне (2.1-кестені қараңыз) және АҚ бойынша әртүрлі жұмыс түрлері үшін техникалық-экономикалық көрсеткіштерді (ТЭК) анықтаудың қолданыстағы әдістемелеріне сәйкес есеп жүргізу үшін әр нақты жұмыс түрінің құны анықталады [75]. Содан кейін алынған мәндер өлшемсіз түрге келтіріледі, мысалы, негізгі шкаланы қолдана отырып [76]. Барлық субъективті көрсеткіштерді (мысалы, сарапшылардың біліктілігі мен жұмыс тәжірибесі) жұмыс құнының көрсеткіштерінде ескереміз.

Осылайша, оптималдылықтың тиісті өлшемін қамтамасыз ету үшін жұмыстың күрделілігі мен шығындарын ескеретін l_{ijk} түріндегі матрицаларды құруға болады. Нәтижелер 2.4-кестеде келтірілген.

Жұптық салыстырудың матрицаларын құру үшін иерархияны талдау әдісі де қолданылды.

2.4-кесте – АОБ АҚ және КҚ ресурстарына инвестициялаудың ұтымдылық өлшемдері мен түрлеріне арналған жұмыстардың еңбек сыйымдылығының матрицалары

k_1 ұтымдылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	АР	БШ	ӨШ
A	23,52	0,65	0,83	0,61
B	15,2	0,41	0,61	0,61
C	12,02	0,21	0,71	0,81
D	17,23	0,51	0,22	0,81
E	22,15	0,21	0,11	0,41
k_2 ұтымдылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	АР	БШ	ӨШ
A	16,72	0,12	0,11	0,51
B	21,32	0,21	0,71	0,11
C	13,89	0,61	0,51	0,81
D	11,22	0,11	0,82	0,21
E	14,34	0,62	0,81	0,22
k_3 ұтымдылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	АР	БШ	ӨШ
A	13,91	0,41	0,71	0,21
B	15,2	0,41	0,61	0,61
C	16,92	0,61	0,81	0,71
D	21,98	0,21	0,81	0,71
E	11,81	0,51	0,31	0,31

Барлық қажетті мәліметтермен популяцияның барлық хромосомалары үшін икемделу функциясының мәндерін табуға болады (2.8-суретті қараңыз).

Егер хромосома шектеулерді (2.3)–(2.5) қанағаттандырмаса, онда оның икемделу функциясының мәні нөлге тең болады.

Зерттеудің келесі кезеңінде ГА-ны іске асыратын бағдарламалық өнім сипатталатындықтан, параграф аясында жоғарыда келтірілген және 2.8-суретте көрсетілген алты хромосоманың бірінші $X_1 = 1011\ \ 0011\ \ 1101\ \ 0011\ \ 1011$ үшін шешімнің тартымдылығын есептеуді ғана егжей-тегжейлі қарастырамыз.

k критерийі үшін (ақпаратты және АҚ саясатын тиімді қорғау нәтижесі ретінде компания үшін бәсекеге қабілеттілік деңгейін арттыру және жаңа нарықтар) $\mu_Q^j(X_1)$ тиістілік функциясын анықтаймыз. Ол үшін матрицаны 2.4-кестенің жоғарғы жағынан (k_1 критерийі үшін) ($X_1 = 1011\ \ 0011\ \ 1101\ \ 0011\ \ 1011$) хромосомаға көбейту керек. Содан кейін нәтижелерді бағандар бойынша қорытындылау керек. Нәтижесінде біз 2.5 түріндегі кестені аламыз.

2.5-кесте – АОБ АҚ және КҚ ресурстарына инвестициялаудың ұтымдылық критерийі және түрлері үшін хромосомаларды трансформациялау матрицалары

Бастапқы мәндер				
A	23,52	0,65	0,83	0,61
B	15,20	0,41	0,61	0,61
C	12,02	0,21	0,71	0,81
D	17,23	0,51	0,22	0,81
E	22,15	0,21	0,11	0,41
Есептеу нәтижелері				
A	23,52	0,00	0,83	0,61
B	0,00	0,00	0,61	0,61
C	12,02	0,21	0,00	0,81
D	0,00	0,00	0,00	0,81
E	22,15	0	0,11	0,41
Бағандар бойынша сома	**57,69**	**0,21**	**1,55**	**3,25**

Осылайша, есептеудің осы қадамының нәтижесінде біз АҚ және КБ бойынша жобаларды бөлу бойынша баламаны іске асыру барысында пайдаланылатын ресурстардың әрқайсысының жиынтық саны туралы мәліметтер аламыз: $Q^{j1}(X_1)=57,69;\ Q^{j2}(X_1)=0,21;\ Q^{j2}(X_1)=0,21;\ Q^{j4}(X_1)=3,25.$ Әрі қарай $\mu_{Q^j}(X_n)$ анықтаймыз.

$Q^{j1}(X_1)=57,69>Q^{j^*}=50$ және $Q^{j4}(X_1)=3,25>Q^{j^*}=3$ болғандықтан, $\mu_{Q^1}(X_1)=\mu_{Q^4}(X_1)=0.$

Мұнда $\mu_{Q^2}(X_1)=\mu_{Q^3}(X_1)=1$, себебі АОБ АҚ және КҚ (РЖ) қамтамасыз ету жөніндегі жобаларға тартылған адам ресурстарының саны және АҚ және ОБИ КҚ (БШ) саласындағы жобаларды басқаруға арналған шығындар шектеудің төменгі шекарасынан аз $A^j=2.$

Ұқсас есептеулер қалған екі k_1 , k_2 және оптималдылық критерийлері үшін басқа критерийлер үшін де жүргізіледі.

Әрі қарай, формуланы (2.11) қолдана отырып, біз 2.1 кестеде қабылданған барлық k_1 , k_2, k_3 критерийтар үшін $F_k(X_1)$ есептейміз, нәтижесінде, келесі мәндер алынады: $F_1(X_1)=27,91$, $F_1(X_1)=44,02$, $F_1(X_1)=53,94$. $F_1(X_1), F_2(X_1), F_3(X_1)$ және $F_{\max k}$ формула бойынша (2.18) есептегеннен кейін по формуле (2.18) $\mu_{F_k}(X_1)$, табамыз, 2.6-кестені қараңыз.

2.6-кесте – $F_k(X_1)$, $F_{\max k}$, $\mu_{F_k}(X_1)$ - есептеу нәтижелері

Ұтымдылық критерийлері	$F_k(X_1)$	$F_{\max k}$	$\mu_{F_k}(X_1)$
k_1	27,91	72,86	0,551
k_2	44,02	79,56	0,412
k_3	53,94	80,54	0,661

Алынған шешімдердің әрқайсысы үшін тартымдылық (2.18) формуласы бойынша Беллман–Заде принципі негізінде есептеледі.

Сонда $\mu(X_1) = \max \min \left\{\mu_F(X_1), \mu_Q^j(X_1)\right\} = 0,$ аламыз, себебі $\mu_{Q^1}(X_1) = \mu_{Q^4}(X_1) = 0.$

Бастапқы популяцияның хромосомалары үшін (2.8-суретті қараңыз) есептеу нәтижелері 2.7-кестеде келтірілген.

X_2, X_3 хромосомалар (2.13)–(2.15) шектеулерді қанағаттандырмайтындықтан, олар үшін икемделу функциясы нөлге тең.

Іріктеу операторы ретінде біз осы процедураны қолданамыз. Алдымен μ_0. популяцияның жалпы икемделуін табамыз, 2.7 кестесіндегі мәліметтерге сәйкес жалпы икемделу: $\mu_0 = 0{,}2 + 0{,}34 + 0{,}5 = 1{,}04.$ құрайды.

Содан кейін біз салыстырмалы μX_n.икемделуді анықтаймыз. Бұл үшін әр шешімге $P(X_n)$.ықтималдық беріледі. $P(X_n)$. мәні оның тартымдылығының барлық шешімдер жиынтығы үшін тартымдылық сомасы қатынасына тең:

$$P(X_n) = \mu(X_n) \Big/ \left(\sum_{n=1}^{m} \mu(X_n)\right) \qquad (2.22)$$

Бастапқы популяцияның хромосомаларына салыстырмалы икемделуді есептеу нәтижелері 2.8-кестеде көрсетілген.

2.7-кесте – Бастапқы популяция хромосомаларының икемделуі

Хромосома нөмірі	Хромосомадағы екілік реттілік	Салыстырмалы икемделу
1	$X_1 = 1011\ \ 0011\ \ 1101\ \ 0011\ \ 1011$	0
2	$X_2 = 0100\ \ 0110\ \ 1101\ \ 0101\ \ 0000$	0
3	$X_3 = 1000\ \ 0000\ \ 1010\ \ 1101\ \ 0000$	0
4	$X_4 = 0111\ \ 0011\ \ 0111\ \ 0001\ \ 1010$	$0{,}2 / 1{,}04 = 0{,}1923$
5	$X_5 = 0101\ \ 1010\ \ 0010\ \ 0110\ \ 1001$	$0{,}34 / 1{,}04 = 0{,}3269$
6	$X_6 = 1111\ \ 0011\ \ 1000\ \ 0101\ \ 1011$	$0{,}5 / 1{,}04 = 0{,}4807$

2.8-кесте – Барлық хромосомалардың нәтижесі

Хромосома	Критерий k_1 (Бәсекеге қабілеттілік деңгейін арттыру және жаңа нарықтар)					Критерий k_2 (Инновацияларды дамыту және бизнес процестерге цифрлық технологияларды енгізу)					Критерий k_3 (АТ шығындарын төмендету)					$\mu(X_n)$
	μ_{Q_i}				μ_F	μ_{Q_i}				μ_F	μ_{Q_i}				μ_F	
	μ_{Q_1}	μ_{Q_2}	μ_{Q_3}	μ_{Q_4}		μ_{Q_1}	μ_{Q_2}	μ_{Q_3}	μ_{Q_4}		μ_{Q_1}	μ_{Q_2}	μ_{Q_3}	μ_{Q_4}		
1	0	1	1	0	0,411	0,491	1	1	1	0,551	0,250	1	1	0,303	0,662	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	1	1	0,8	0,2	0,521	1	1	0,9	1	0,481	1	1	0,303	0,60	0,60	0,2
5	1	1	1	1	0,461	1	1	1	1	0,412	1	1	1	1	1	0,34
6	1	1	1	0,6	0,582	1	1	1	1	0,661	0,50	1	1	1	1	0,5

Зерттеу барысында пропорционалды іріктеу (немесе рулетка схемасы) қолданылды. Пропорционалды таңдау хромосомаларды ата-ана ретінде таңдау ықтималдығын анықтауға мүмкіндік береді. Іріктеу хромосомалардың салыстырмалы бейімділігі негізінде жүзеге асырылады. Схема «рулетка» деп аталды, өйткені процесс барысында сенімділік аралығы ата-аналарды таңдау рулетка секторын таңдауға ұқсас.

Рулетка *m* бір рет іске қосылады, яғни бастапқы популяция үшін шешімдер санына пропорционалды.

$P(X_n)$ ықтималдық, шын мәнінде, *n*-шешім үшін рулетка секторының көлеміне сәйкес келеді.

Бұдан әрі орындалады: іріктеу жасаймыз. Таңдау процесінде барлық шешімдер ауыстырылады. Таңдау үшін интервалда біркелкі таралуы бар кездейсоқ *m* сандарды құру керек (0,1). Содан кейін өрнектің көмегімен жаңа шешімдер жиынтығын құруға болады:

$$X_n^{new} = \begin{cases} X_n, if\ W_n < P(X_n); \\ X_{n+1}, if\ P(X_n) < W_n < P(X_{n+1}), \end{cases} \quad (2.23)$$

мұнда $n = 1,2,...,m.$ үшін $W_n -$ кездейсоқ шешімдер саны.

2.9-кесте – Рулетка схемасын қолдану нәтижесінде пайда болған популяция

Нөмір	Популяция хромосомасындағы екілік реттілік	Салыстырмалы икемделу
1	1111 0011 1000 0101 1101	0,5
2	0101 1001 0010 0110 1001	0,34
3	1111 0011 1000 0101 1101	0,5
4	0111 0011 0111 0001 1010	0,2
5	0101 1001 0010 0110 1001	0,34
6	1111 0011 1000 0101 1101	0,5

Мысалы, 2.9-кестеде көрсетілген популяция алты кездейсоқ сандардың көмегімен құрылды.

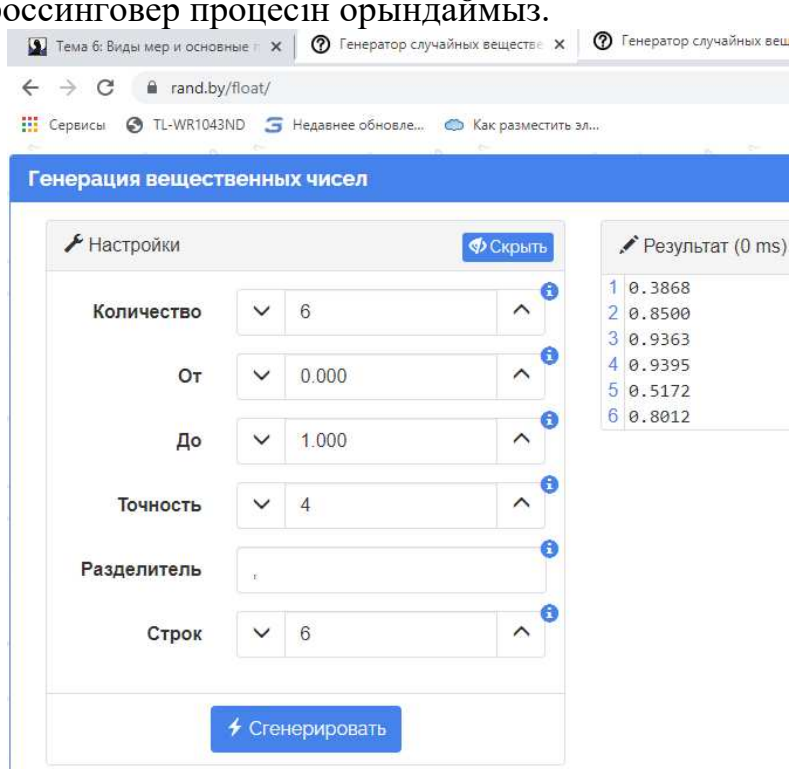
Таңдау операторын қолдану нәтижесінде жаңа жиынды аламыз. Кроссинговерге қатысатын хромосомаларды таңдау үшін келесі қадамдарды орындау қажет:

1-қадам) Алты кездейсоқ санды өңдеу, генерациялау үшін онлайн қызметті пайдаланған, 2.12-суретті қараңыз.

2-қадам) Кездейсоқ сан 0,8-ден аз болса, біз таңдаймыз деген ережеге сүйене отырып хромосомаларды таңдаңыз. Бұл мән комбинацияның ықтималдығынан $0{,}8$ аз болғандықтан қабылданады.

3-қадам) Хромосомаларды таңдағаннан кейін кездейсоқ кроссинговер нүктесін таңдаймыз, мысалы, кездейсоқ сандарды онлайн режимінде өңдеу қызметін қолдана отырып.

3-қадам) Кроссинговер процесін орындаймыз.



.12-сурет – Кездейсоқ сандар генераторының онлайн жұмысының мысалы

Генерация нәтижесінде мұндай кездейсоқ сандар интервалда алынды (0,1): $x_1 = 0{,}7532; x_2 = 0{,}9307; x_3 = 0{,}5325; x_4 = 0{,}1211; x_5 = 0{,}1732; x_6 = 0{,}8345.$

Сонда ата-аналық хромосомалардың жұптары $X_1 - X_3$ және $X_4 - X_5$ болады $X_1 - X_3$ жұбы үшін қиылысу нүктесі 12. $X_4 - X_5$ жұбы үшін - 8. Қиылысу нүктелерінен кейін орналасқан хромосомалардың бөліктерінің (яғни биттер) орнын өзгертеміз. Кроссинговер процесі және ұрпақ алған нәтиже 2.10-кестеде көрсетілген.

.2.10-кесте – Кроссинговер процесі

Ата-аналар	Кроссинговер			Ұрпақтары
$X_1 - X_3$				
1111 0011 1000 01011101	1111 0011 1000 ~ 01011101	→	1111 0011 1000 ~ 01011101	1111 0011 1000 01011101
1111 0011 1000 01011101	1111 0011 1000 ~ 01011101	→	1111 0011 1000 ~ 01011101	1111 0011 1000 01011101
$X_4 - X_5$				
0111 0011 0111 0001 1010	0111 0011 ~ 0111 0001 1010	→	0111 0011 ~ 0010 0110 1001	0111 0011 0010 0110 1001
0101 1001 0010 0110 1001	0101 1001 ~ 0010 0110 1001	→	0101 1001 ~ 0111 0001 1010	0101 1001 0111 0001 1010

Егер кроссинговер процесінде қалыптасқан ұрпақтар (2.13)–(2.15) шектеулерді қанағаттандырса, онда біз оларды ата-аналардың орнына қайта жазамыз. Егер шектеулер (2.13)–(2.15) қанағаттандырылмаса, онда біз ата-аналық шешімдерді өзгеріссіз қалдырамыз. Тиісінше, хромосомалардың жаңа ұрпағы 2.11-кестеде көрсетілгендей болады.

2.11-кесте – Жаңа ұрпақ

Нөмірі	Популяция хромосомасындағы екілік реттілік	Салыстырмалы икемделу
1	1111 0011 1000 0101 1101	0,5
2	0101 1001 0010 0110 1001	0,34
3	1111 0011 1000 0101 1101	0,5
4	0101 1001 0111 0001 1010	0,2
5	0101 1001 0010 0110 1001	0,34
6	1111 0011 1000 0101 1101	0,5

Мутацияның ГА-да іріктеу процесіне қалай әсер ететінін қарастырайық. сәйкес, мутация – бұл хромосома биттерінің бірінің инверсиясы. Бұл бит те кездейсоқ таңдалады. Мутация операторы мутацияның төмен ықтималдығын ескере отырып жұмыс істеді делік. Мысалы, үшінші хромосоманың 17-ші битін

мутациялады: Популяцияның үшінші хромосомасындағы бастапқы екілік реттілік: 1111 0011 1000 0101 1101

Мутациядан кейінгі популяцияның үшінші хромосомасындағы екілік реттілік: 1111 0011 1010 0101 0101

Бұл хромосоманың икемделуі да артты. Егер бастапқыда ол 0,5 болса, мутациядан кейін ол 0,56 болды. Осылайша, ГА жұмысының нәтижесінде пайда болған популяция 2.12-кестедегідей болады. Осымен ГА циклы аяқталды. Циклдар саны жұмыста қарастырылған мақсатты функцияларды ұтымды шешудің дәлдігіне әсер етеді, сондықтан жұмыстың келесі тарауларында есептеулерді автоматтандыру үшін ГА тарауында сипатталған БҚ әзірлеуге назар аударылады.

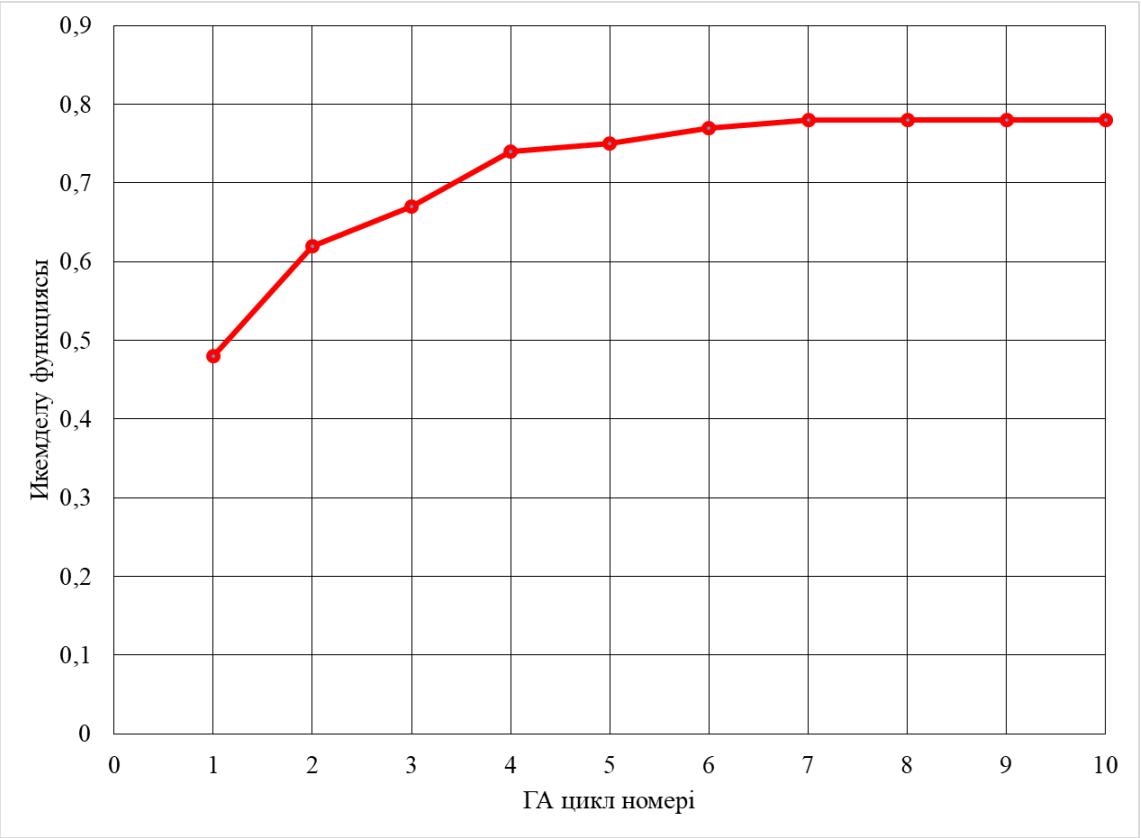
2.12-кесте – Алынған популяция

Нөмірі	Популяция хромосомасындағы екілік реттілік	Салыстырмалы икемделу
1	1111 0011 1000 0101 1101	0,5
2	0101 1001 0010 0110 1001	0,34
3	1111 0011 1010 0101 0101	0,56
4	0101 1001 0111 0001 1010	0,2
5	0101 1001 0010 0110 1001	0,34
6	1111 0011 1000 0101 1101	0,5

2.8 және 2.12-кестелерінің деректерін салыстырмалы талдаудан көрініп тұрғандай, тіпті бір ғана итерация кезінде популяция сапасы екі еседен астам өсті.

Қазіргі және алдыңғы қадамдардағы икемделу функциясының ең үлкен мәндерінің арасындағы айырмашылық 0,01-ден аз болған кезде алгоритм тоқтайды, 2.7-суретті қараңыз. Бірінші циклден кейін бұл айырмашылық 0,5 болды, жаңа цикл қажет. Тест барысында $0{,}78 \approx 0{,}8$ деңгейінде икемделу функциясының ұтымды мәнін алу үшін ГА 7-ден 9-ға дейін цикл өтті.

2.13-суретте жобаланған ГА үшін икемделу функциясының (икемделу функциясының) өзгеру кестесі көрсетілген. 8 циклден кейін икемделу функциясы өзінің мағынасын сақтайды және ГА жұмысын жалғастырудың мәні жоқ [77].



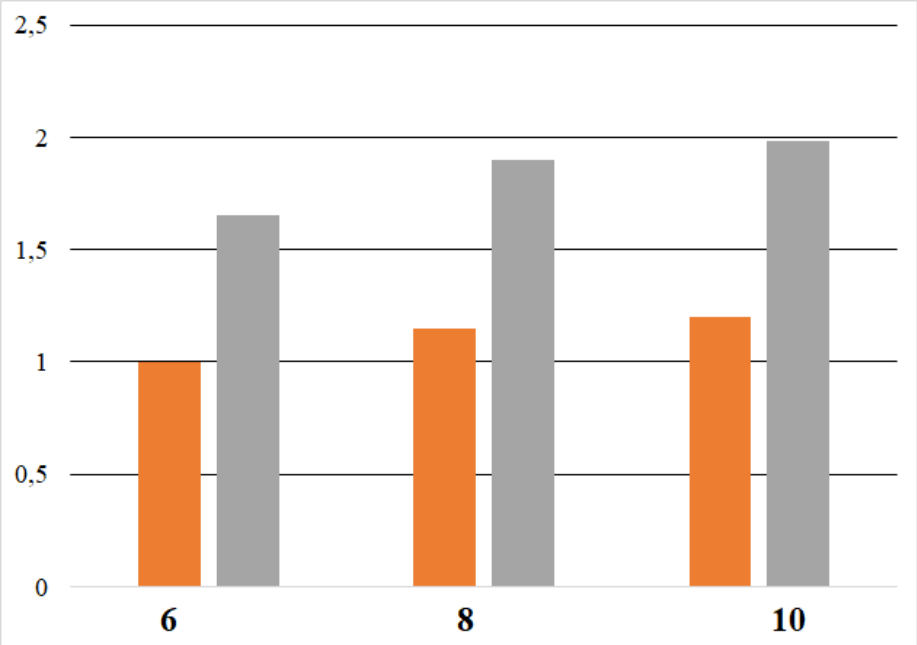
2.13-сурет – Әзірленген құрама ГА үшін икемделу функциясының өзгерту кестесі

Алынған шешімді тексеру үшін қарапайым сұрыптау әдісін қолдана отырып, есепті шешудің бақылау есептеулері жасалды. Қарапайым сұрыптау аясында хромосомалардың барлық мүмкін мәндері үшін икемделу функциялары есептелді. Хромосомалардың жалпы саны бойынша 20 айнымалыдан тұратын шешім матрицасының мүмкін күйлерінің саны бірден мүмкін болатын шешімдердің 50%-дан астамы (2.13) - (2.15) шектеулерді қанағаттандырмайтындығын атап өтті. Осы баламалар үшін есептеулер жүргізілген жоқ. Қалған хромосомалар үшін икемделу функциясы іріктеліп алынды. Екі әдіс те ұқсас нәтиже берді, бірақ шешім табу үшін қарапайым іздеу үшін шамамен 65% көп уақыт қажет болды, 2.14-суретті қараңыз. Уақыт шкаласы шартты бірліктерде ұсынылған (мысалы, минуттарда немесе он минутта, өйткені әртүрлі процессорлары бар ЖК қолданған кезде есепті шешу уақыты дұрыс болмауы мүмкін). Осылайша, икемделу функциясы 0,8 мәніне сәйкес келетін шешім ұтымды шешу есебінің шешімі болады.

Осылайша, ГА көмегімен алынған шешімге сүйене отырып, келесі қорытынды жасауға болады:

компания (кәсіпорын) өзінде бар ресурстарды ескере отырып, ақпаратты қорғаудың кешенді жүйелерін өрістету жөніндегі жұмыстарды ұйымдастырған жөн, өйткені бұл жұмыстар қорғаныс тарабы мен шабуыл жасаушылардың ресурстарының әртүрлі үйлесімдері кезінде АОБ осалдығын сипаттайтын мақсат функцияда (2.10) пайдаланылатын *a* параметр мәнінің 80%-ына дейін қамтамасыз етеді;

кешенді АҚҚ-ға ғана бөлінетін ресурстарды одан әрі қайта бөлу ұсынылмайды, өйткені бұл АОБ-дағы ақпараттың осалдығын одан әрі төмендетуге әкелмейді.



2.14-сурет – Әзірленген ГА көмегімен және қарапайым сұрыптау әдісі үшін 6,8,10 хромосомасына есепті шешуге арналған уақыт шығындарын салыстыру диаграммасы (ш.б.-де)

Оң нәтижені барынша арттыру үшін *а* жұмыс түрінің шеңберінде (кешенді АҚҚ жобалау, әзірлеу және өрістету): сәйкестендіру және аутентификациялау; қолжетімділікті басқару; ақпаратты машиналық тасығыштарды қорғау; басып кіруді анықтау; виртуалдау ортасын қорғау; және т.б. жүйелерге қаражат инвестициялау қажет. Бұл қорытынды $x_{11} = x_{12} = x_{14} = 1$.ГА-ның жұмысын көрсету үшін сынақ мысалына негізделген. А $x_{13} = 0$ болғандықтан, бұл ұсыныс АОБ АҚ және КҚ саласындағы жобаларды басқаруға қаражат салуды болдырмау болып табылады, өйткені бұл іс-шаралар күрделілік-ұтымдылық қатынасы бойынша шектеулерді қанағаттандырмайды. Басқа бастапқы деректер үшін жағдай басқаша болуы мүмкін және бұл бағыт АҚҚ мен КҚ-ға инвестиция салу басымдыққа ие болады.

Сол сияқты, 2.1-кестесіндегі тізімнен басқа жұмыстар үшін ойлау тізбегін құруға болады. Егер бастапқы деректерде көрсетілген ресурстардың әр түрін қолдануды қарастыратын болсақ, онда тек адам ресурсының артықшылығы бар деп айтуға болады. Қалған ресурстар белгіленген анық емес шектеулер ауқымында болады.

Мұндай жүйелерді таңдау бойынша көп критерийлі есепті шешудің модельдері мен әдістерін азаматтық авиация жүйесін қолдану негізінде де ұйымдастыруға болады. Диссертацияның келесі тараулары осы зерттеулерге арналған. Бұл есепті шешу көбінесе n параметрдің шекаралық көрсеткіштерін

анықтауға бағытталған, өйткені көптеген түйіндерден тұратын көп контурлы жүйелерді құруға келгенде қорғаныс өнімділігі соған байланысты болады. Әрбір мұндай тораптарда ақпарат өңделуі, сақталуы, берілуі, жаңаруы мүмкін. Тиісінше, қорғаныс тараптарының ресурстары шектеулі немесе минималды болған жағдайда қорғаныс құралдары мен тетіктерін таңдау жеке есеп болып табылады.

2.3. 2 тарау бойынша қорытындылар

Зерттеу нәтижесінде АОБ объектілерінде ақпараттық ресурстардың осалдығы мен қауіптерді іске асырудан келтірілген залалды сипаттайтын модельдің мақсатты функциясын таңдау негізделген.

Бөлшек-сызықтық функциялар материалдық тасымалдаушыларда сақталатын ақпараттың осалдығын сипаттайды, мұнда ақпаратты қорғауға, сондай-ақ ұйымдастырушылық және инженерлік-техникалық іс-шараларға және қорғаныс құралдарына бөлінетін ресурстардың ұлғаюы, қорғаныс жақтары ресурстары мәндерінің бастапқы аймағында осалдықтың монотонды, пропорционалды түрде азаюына және нәтижесінде АОБ үшін келтірілген залалдың азаюына әкеледі.

Бөлшек-сызықты емес функциялардың кедергілерді жеңу үшін айтарлықтай ресурстар қажет болатын компьютерлік жүйелерде таратылатын ақпараттың қасиеттерін көрсететіні анықталды.

Мақсатты функцияға кіретін және АОБ-дағы ақпаратты қорғауды қамтамасыз ету жөніндегі жұмыстар тізбесіне тәуелді ұтымды $a, n,$ параметрлерді (бұл параметрлер АОБ үшін АҚҚ шығындарының өнімділігіне немесе жалпы жағдайда нақты АҚҚ тиімділігі көрсеткіштерінің және оларды сатып алуға, қызмет көрсетуге, жаңғыртуға арналған шығындар көрсеткіштерінің арақатынасына сәйкес келеді) іздеу есебін шешу үшін және кешенді АҚҚ өрістету, АҚ (АҚОЖ) қамтамасыз ету жүйесін жетілдіру және т.б.) алғаш рет жаңғыртылған генетикалық алгоритмді (ГА) пайдалану ұсынылды. Жаңғыртылған ГА-да қолданыстағыларға қарағанда, анық емес қатынастармен кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді ұтымды шешудің көп критерийліесебін шешу үшін Беллман-Заде қағидаты қолданылды. Бұл АОБ құрамындағы компоненттердің осалдықтарын төмендетуге бағытталған іс-шаралармен байланысты жұмыстарға ресурстарды бөлуді ұтымды шешуге және шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда АОБ қорғанысының берілген мәндеріне қол жеткізуді қамтамасыз ететін ресурстар көлемінің әртүрлі нұсқаларын модельдеуге мүмкіндік береді.

3 МОДИФИКАЦИЯЛАНҒАН ГЕНЕТИКАЛЫҚ АЛГОРИТМДІ ҚОЛДАНУ НЕГІЗІНДЕ АҚПАРАТТЫ ҚОРҒАУ ҚҰРАЛДАРЫН ОРНАЛАСТЫРУДЫ ҰТЫМДЫ ШЕШУ БОЙЫНША ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ

3.1. Ақпаратты қорғау тарапының ресурстарын іріктеу, ұтымды шешу және қайта бөлу есебін шешу үшін генетикалық алгоритмді дамыту

Әртүрлі АҚИ мен олардың ақпараттық-коммуникациялық жүйелеріне (АКЖ) сәтті іске асырылған кибершабуылдардың саны мен күрделілігіне қарай қорғаныстың барлық контурларында АҚ және КҚ кешендерінің құрамын қалыптастырудың сапалы жаңа рәсімдеріне қажеттілік артады. АКЖ КҚ тиімді контурларын қалыптастырудың тұрақты есебі АҚҚ және КҚ құрамын ұтымды шешу есеплері бойынша көптеген зерттеулер жүргізгенін байқаймыз. Бұл зерттеулер, ең алдымен, көп критерийлі ұтымды шешу есептерін шешуге байланысты сұрақтарға жауап беруге арналған, олар келесідей қасиеттерге ие: жеке АҚҚ-ны қолданудың рұқсат етілген аймағының күрделі конфигурациясы; қарастырылған функциялардың көп экстремалдылығы; функциялардың алгоритмдік тапсырмасы және т. б. Сонымен қатар, тиімді көп тізбекті КҚ жүйелерін құрудың нақты есептерінде шешімдер сирек бір критерий бойынша бағаланады. Сондықтан, мұндай есеплерде қолайлы парето-ұтымды шешімдерді табу ғана емес, сонымен қатар шешім қабылдауш тұлғаларға (ШҚТ) АКЖ КҚ тиісті контурлары бойынша АҚҚ-ны объективті таңдауды ұсыну үшін алынған көптеген нұсқаларды жақындату маңызды. АКЖ-ға деструктивті әсер ету әрекеттері санының өсуі жағдайында ақпаратты қорғаудың көп контурлы жүйелерін құрудың жоғарыда аталған есептерін шешу тек классикалық ұтымды шешу процедураларын ғана емес, сонымен қатар көптеген күрделі есептерді шешуде тиімді екендігі дәлелденген генетикалық алгоритмдерді (ГА) қолдануды талап етеді [78].

ГА тиімділігі олардың параметрлерін мұқият реттеу және бақылау арқылы анықталады. Бұл ГА-ны АКЖ-контурлары бойынша АҚҚ тиімділігін қарапайым инженерлік есептеулерде қолдануды біршама қиындатады. Алайда, егер АКЖ арналған АҚҚ құрамын таңдау бойынша дәстүрлі көп критерийлі ұтымды шешу есебінен басқа, тәуекелдердің шамасын, сондай-ақ нақты активтер үшін (деректер базасы, білім базасы, пошта, сайт және т.б.) іріктелген АҚҚ құндық көрсеткіштерін қарастырса, ГА-ны қолдану әбден орынды болады. Шешімді іздеу процедурасы шешім қабылдауды қолдаудың интеллектуалды жүйелерінің (ШҚҚЖ) әлеуетін пайдаланса, тиімдірек болуы мүмкін, олардың есептеу ядросы іс жүзінде ГА-ны қолдануға негізделген.

1 және 2 ГА тарауларында көрсетілгендей, көп критерийлі есептерді ұтымды шешу кезінде қолданылатын іздеу эволюциялық әдістерінің нұсқалары болып табылады. Соңғы бірнеше жылда осы саладағы зерттеулерге көптеген жұмыстар арналды. Ең жақсы шешімді табу үшін авторлар өздерінің мақсатты функциясын қолданды. Жұмыста ұсынылған шешімдер іс жүзінде қалай және қай жерде нақты қолданылғаны көрсетілмеген.

[79] еңбектерінде екі топқа жатқызуға болатын ГА зерттелді. Бірінші топта екілік кодталған ГА зерттелді. Екінші топта, тиісінше, қолданыстағы кодталған ГА. Бұл жұмыстар бірінші топта рұқсат етілген шешімдер жиынтығында экстремалды мәнді іздеудің жоғары тиімділігіне қол жеткізуге болатындығын көрсетеді.

[80] еңбектерінде модификацияланған ГА-ны мұндай көп критерийлі есептерді ұтымды шешуді қолдану ерекшеліктері қарастырылды. ГА-ның стандартты ГА-дан салыстырмалы икемделу функциясымен айырмашылығы мынада: алгоритм жұмыс істеп тұрған кезде икемделу функциясы ретінде АҚҚ тиімділігінің қосындысы қолданылмады, ол іс жүзінде хромосома болды, бірақ АҚҚ-ның шектеуші сипаттамаларына ұтымдылық қатынастарының қосындысы немесе ұтымдылық коэффициенті қолданылды. ГА-ның ұқсас модификациясы іс жүзінде стандартты ГА және сараң алгоритмнің бұзылуы болып табылады.

АКЖ-ғқа арналған АҚҚ құрамын таңдауды ұтымды шешу есебін көп таңдаумен байланысты есептердің вариациясы ретінде қарастыруға болады [81]. Бұл жұмыстарда АКЖ (КББ) контурларының компоненттерін орналастыруды ұтымды шешу рюкзак комбинаторлық тапсырмасының белгілі бір модификациясы ретінде қарастырылады. Бұл тәсіл шешімді тұжырымдау мен түсіндірудің қарапайым формалдануымен ерекшеленеді. Алайда, авторлар генетикалық, қарапайым сұрыптау, динамикалық бағдарламалау және т.б. сияқты шешім алгоритмдерін толық шешуді және салыстыруды ұсынған жоқ.

Алайда, мультипликативті рюкзак туралы тапсырма басқа кластарындағы заттармен бір АҚҚ класындағы заттарды ауыстыруға байланысты барлық мүмкіндіктерді көрсетпейтінін ескертеміз. Алайда, ауыстырылатын заттар балама функцияларды орындайды. Сондықтан объектілердің жалпы құнының орнына көптеген мақсаттарды көрсететін функцияны енгізу қажет. Бұл «рюкзактағы» заттардың өзара алмастырылуын немесе баламалылығын көрсету үшін жасалады.

КҚ және АҚ қамтамасыз ету тұрғысынан АКЖ инфрақұрылымы 3.1-суретте көрсетілген.

Әдепкі бойынша, АКЖ түйіндерінде стандартты АҚҚ орнатылған: антивирустар; брандмауэр; құралдар: 1) басып кіруді анықтау 2) криптографиялық АҚ; 3) қол жеткізуді шектеу; 4) тұтастықты бақылау; 5) аутентификация және т. б.

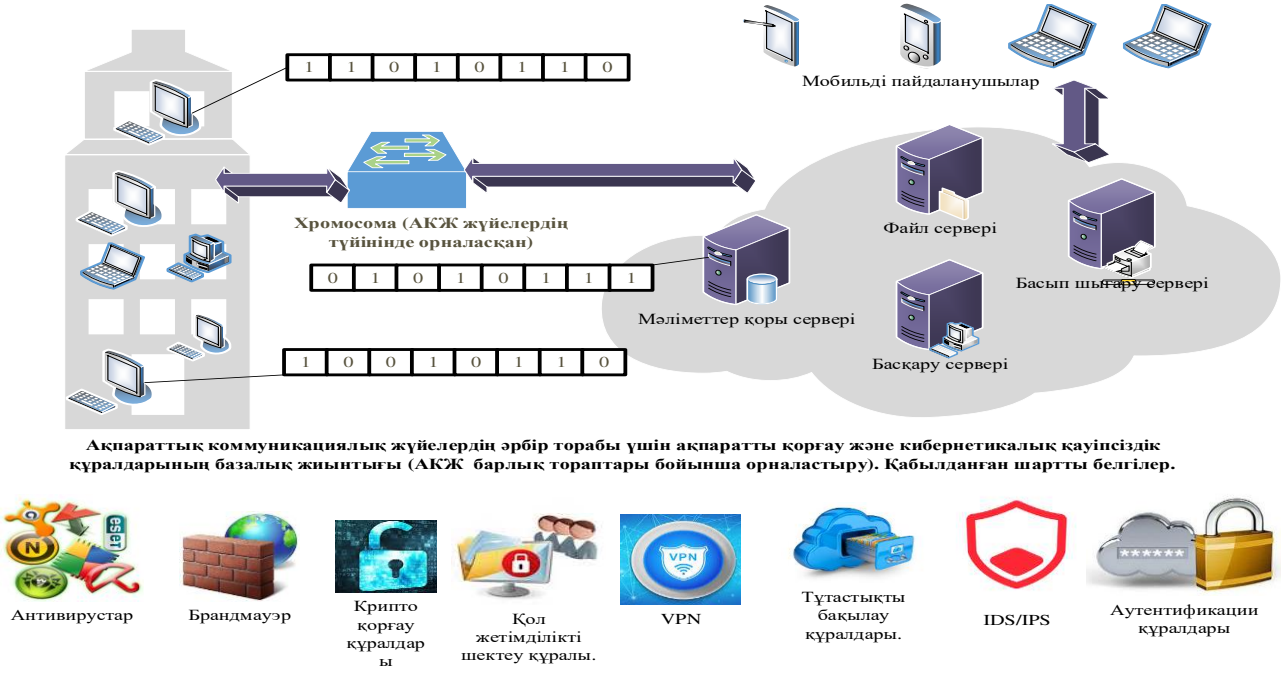
Әрине, нақты АКЖ үшін тізім жеткіліксіздікке байланысты толықтырылуы немесе артықтығына байланысты қысқартылуы мүмкін.

NIST ұсыныстарында АКЖ-да КҚ және АҚ қамтамасыз етудің архитектурасы, негізгі осалдықтары және ерекшеліктері егжей-тегжейлі сипатталған. Алайда, бүгінгі күні нақты АКЖ-ның барлық ерекшеліктерін, КҚ-ны қамтамасыз ету тетіктерін талдауды және қауіптердің салыстырмалы спектрін ескере отырып, АКЖ түйіндері бойынша АҚҚ мен КҚ орналастырудың ұтымды нұсқасын іздеу процесінде біржақты шешім қабылдауға қабілетті әмбебап тәсіл жоқ екенін ескереміз. Нәтижесінде, мұндай тәсілді құру туралы есеп туындайды. Бұл жағдайда алынған шешім келесі мүмкіндіктермен ерекшеленуі керек:

1. Нақты АКЖ құрылымына негізделген ақпараттық және КҚ контурларының әртүрлі нұсқаларын жобалау мүмкіндіктері.

2. Әртүрлі кластардың нақты қауіп-қатерлеріне қарсы тұру қажеттіліктеріне негізделген АҚҚ таңдау мүмкіндіктері.

3. Шабуыл механизмдерінің эволюциясына сүйене отырып, АҚҚ және КҚ жиынтықтарын іріктеу және ұтымды шешу алгоритмін бейімдеу (эволюциялық) мүмкіндігімен. Бұл, өз кезегінде, АКЖ түйіндері үшін АҚҚЖ таңдаудың нақты әдістерін қолдануға мүмкіндік бермейді.



3.1-сурет – КҚ қамтамасыз ету тұрғысынан АКЖ АОБ инфрақұрылымы

3.1-суретте көрсетілген АҚҚ тізбесі толық емес. Бизнес-процестердің ерекшелігіне, АОБ-дағы ақпараттық ресурстардың күрделілігіне байланысты бұл тізім кеңеюі мүмкін. Қорғаудың аппараттық-бағдарламалық құралдары, мысалы, SIEM системалар (АҚ оқиғаларын (дабылдарын) нақты уақытта талдау процестерін қамтамасыз ететін және осы оқиғаларға айтарлықтай залал басталғанға дейін ден қоюға мүмкіндік беретін), (инсайдерлік ақпараттың жария болуын болдырмау мақсатында қызметкерлердің іс-әрекеттерін қадағалауға және талдауға мүмкіндік беретін) және т. б., сондай-ақ ұйымдастырушылық және басқа да шаралар есебінен, мысалы, КҚ бойынша мерзімді оқу-жаттығулар өткізу, персонал жұмысын бақылау жүйелері есебінен айтарлықтай кеңейтілуі мүмкін.

Жоғарыда айтылғандарға сүйене отырып, АКЖ-ға арналған АҚҚ-ның ұтымды конфигурациясын (бұдан әрі – жиынтық) таңдау процесінде көп таңдау есебін (мысалы, антивирустар, желілік экрандар, басып кіруді анықтау құралдары және т.б.) шешу үшін ГА қолдану мүмкіндігін қарастырамыз.

Біз шешімді кодтаудың келесі табиғи әдісін қолданамыз. Бастапқыда барлық құралдар, ал біздің жағдайда тиісті кластара жатқызылған АҚҚ

тақырыпты ұсынудың екілік форматында нөмірленеді. Содан кейін әр хромосоманы $(x_1, x_2, ..., x_n)$ вектор түрінде көрсетуге болады. Бұл векторда егер бұл ақпаратты қорғау құралы АКЖ түйінінде болса (рюкзак немесе мультирюкзак үшін бөлім) x_i элемент (яғни, *i*-ген) 1-ге тең (бірлік) немесе қарама-қарсы жағдайда - 0. Әрбір $(x_1, x_2, ..., x_n)$ булдік вектордың рұқсат етілген шешімді кодтай бермейтіні даусыз. Бұл АКЖ түйініндегі элементтер жиынтығына (АҚҚ) шектеулердің болуымен байланысты. Мысалы, пайдаланушылардың мобильді құралдарында (ноутбуктер, планшеттер және т.б.) басып кірулерді анықтау құралдарын олардың қымбат болуына және есептеу ресурстарына сұранысқа байланысты олардың толық ауқымды нұсқасында орналастырудың мәні жоқ. Сонымен қатар, түйіннің сыйымдылығы қаражаттың жалпы құнымен шектеледі (рюкзактың сыйымдылығы немесе біздің жағдайда интегралды көрсеткіш (ИнК) (АҚҚ), олар сол жерде орналасуы мүмкін. Сонымен қатар, жұмыстың екінші тарауында айтылған ресурстарды қайта бөлуге байланысты шектеулерді ескеру қажет.

Әрбір осы АОБ үшін мұндай есеп қоюдағы икемделу функциясы осы АОБ есепті шешудің сенімді нұсқасына «жақындық» дәрежесін сипаттайды. Икемделу функциясының мәні неғұрлым көп болса, шешім қалаған максимумға жақын болады.

Содан кейін түйінге арналған икемделу функциясын (АКЖ үшін АҚҚ орналастыру нүктесі) келесідей пайдалануға болады:

$$f(x_1, x_2, ..., x_n) = \sum_{i=1}^{n} w_i \cdot x_i,$$

мұнда w_i – сапа индексі немесе белгілі бір АҚҚ үшін қажетті мақсаттарға қол жеткізу дәрежесі деп аталатын класс немесе нақты АҚҚ-ның интегралдық көрсеткіші (ИнК) [82].

Сондай-ақ, ИнК белгілі бір АҚҚ-ның маңызды сипаттамаларының сапасының жалпыланған көрсеткіші ретінде түсіндірілуі мүмкін. Интегралды көрсеткіш АОБ үшін АҚҚ-ға арналған шығындардың *a,b,n* өнімділік параметрлерімен немесе жалпы жағдайда нақты АҚҚ-ның ұтымдылық көрсеткіштері мен оларды сатып алуға, қызмет көрсетуге, жаңғыртуға арналған шығындар көрсеткіштерінің арақатынасымен тікелей байланысты.

Әзірленген алгоритмде сапа индексі немесе белгілі бір АҚҚ үшін қажетті мақсаттарға қол жеткізу дәрежесі ИнК АҚҚ ретінде қабылданды [83]. Авторлар ИнК-ті белгілі бір АҚҚ-ның маңызды сипаттамалары сапасының жалпыланған көрсеткіші ретінде түсіндіреді. Бұл ретте, ИнК АҚҚ параметрлерінің бөлінген жеке көрсеткіштер кеңістігіндегі мінсіз сипаттамаларға жақындық дәрежесі ретінде есептелген деп есептейміз [83, б.150-154]. АҚҚ ИнК есептеу үшін, әдетте, келесі тәуелділікті қолданамыз:

$$IND_j = \sum_{i=1}^{k} \beta_i \cdot a_{ij}, \qquad (3.1)$$

мұнда β_i – i-ші АҚҚ бағалау үшін пайдаланылатын өлшемнің салмағы (мысалы, файерволдар үшін мынадай өлшемдерді пайдалануға болады: ішкі шабуылдардан қорғауға арналған брандмауэр тесті; сыртқы шабуылдардан қорғауға арналған брандмауэр тесті; осал қосымшаларға жасалған шабуылдардан қорғауға арналған дербес IDS/IPS тесті; құжаттаманың болуы және т. б.);

a_{ij} – шабуылдардың әр класы үшін түйіннің берілген қорғаныс деңгейіне жету дәрежесі;

k – АКЖ түйінінің белгілі бір түріне арналған АҚҚ кластарының саны.

АОБ-нің тиісті контурларына таралған ақпаратты қорғау жүйелері мен жеке АҚ құралдарын талдай отырып, жұмыстың алдыңғы тарауларында көрсетілгендей, барлық объектілер жүйе үшін бірдей мәнге ие емес және бірдей дәрежеде қорғалуы керек екенін атап өткен жөн. Бұл жағдай генетикалық алгоритмді көп критерийліесеп үшін қолдану тұрғысынан АҚҚ ИнК есептеуге өз ерекшеліктерін жүктейді.

Шынында да, АКЖ-де орналасқан кейбір объектілердің жұмыс істеуі бизнес-процестерді жүзеге асыру үшін өте маңызды, мысалы, дерекқор серверлері немесе қосымшалар сервері. Олардың істен шығуы дереу барлық АКЖ АОБ-қа әсер етеді және төтенше жағдайларда оның қабылданбауына әкеледі. Басқа жүйелер онша маңызды емес, олардың бүкіл АОБ-тің жұмысына әсер ету дәрежесі онша үлкен емес. Мысалы, кәдімгі компьютердің істен шығуы бизнес-процестерді толығымен тоқтатуға әкелмейді. АКЖ-тің маңызды және маңызды емес түйіндері үшін олардың қорғаныс құралдары қажет болса да, оларда орналасқан ақпараттық ресурстардың маңыздылығы мен сыншылдығына байланысты оларды қайта бөлу де маңызды рөл атқарады. Осыған байланысты ЖТС есептеу нақты АҚҚ аса маңызды параметрлерінің сапа сипаттамаларын жалпылаудың қарапайым процедурасынан аса күрделі есеп болып табылады.

Демек, интегралды көрсеткішті сапалы сипаттау үшін осы қорғаныс құралын орнату жоспарланған АОБ түйінінің барлық қасиеттерін ескеру қажет. Атап айтқанда, мыналарды ескеру қажет: түйіннің маңыздылығы; АКЖ-да осы түйіннің маңыздылығы; түйін үшін қорғаныс шараларын жүзеге асыру әдісі.

Бұл тізімде «сыншылдық» қасиеті басым болады. Ол түйіннің бүкіл АКЖ-ға әсер ету дәрежесін анықтайды.

«Маңыздылық» сияқты қасиет олардың жалпы ИнК-дағы нақты АҚҚ параметрлерінің салмағын анықтайды. Яғни, бұл интерпретациядағы маңыздылық ақпараттық қауіпсіздік жүйесінің функцияларының қайсысының кему ретімен түйін үшін маңыздырақ, ал қайсысы маңызды емес екенін ғана анықтайды. Осылайша, түйіндегі АҚҚ-ның «маңыздылығын» анықтау үшін олардың функционалдық сипаттамаларын басымдықтардың маңыздылығына қарай орналастыру керек. Мысалы, антивирустық БҚ үшін ИнК-ны сипаттауда зиянды БҚ анықтау көрсеткіші маңыздырақ, ал антивирустық сигнатураларды

күніне 2 немесе 1 рет жаңарту жиілігі онша маңызды емес. «Түйін үшін қорғау шараларын іске асыру» қасиеті тиісті АҚҚ параметрінің жай-күйі туралы ағымдағы деректердің болуын немесе болмауын анықтайды. (3.1) өрнектегі АҚҚ жиынтығындағы заттарды сапалы бағалау үшін β_i нақты мән немесе шамамен қолданылуы маңызды емес. Бұл β_i параметр ең алдымен β_i сандық бағалау мен объектінің біржақты сәйкестігін жүзеге асыратындығына байланысты. Іс жүзінде, объектілерді бағалау процесінде бағалау көбінесе шындыққа қарағанда пессимистік сипатта болады. Осылайша, интегралды көрсеткіштің β_i параметрі мен мәнін анықтаған кезде бағалау үшін β_i аралық бағалауды қолданған дұрыс деп айтуға болады.

ГА үшін $\tau(\beta_i)$ нақты мәндерді таңдағанда, жиынтыққа кіретін заттың әртүрлі сапалық бағалары арасындағы салмақ арақатынасын қалыптастыруға баса назар аударылады. Тиісті аралықтың шекарасындағы $\tau(\beta_i)$ мәндердің өзгеруі жиынтықтағы заттың сапалық бағасын қатайтады немесе керісінше әлсіретеді.

Жоғарыда айтылғандарды ескере отырып, АҚҚ ИнК келесі тәуелділіктер арқылы есептеуге болады:

$$IND_j = \sum_{i=1}^{k} \tau(\beta_i) \cdot a_{ij}, \qquad (3.2)$$

мұнда $$\tau(\beta_i) = \begin{cases} \tau_1, \beta_i \in \lfloor b_{1_1}, b_{1_2} \rfloor \\ \tau_2, \beta_i \in \lfloor b_{2_1}, b_{2_2} \rfloor \\ \quad \ldots \\ \tau_j, \beta_i \in \lfloor b_{j_1}, b_{j_2} \rfloor \end{cases},$$

b_{j_i}, b_{j_n} – АКЖ түйініндегі АҚҚ жиынтығындағы пәнді бағалау шкаласының сол және оң жақтары.

Осылайша, (3.2) қатынасы объектіні бағалаудың сандық баламалары жиынындағы β_i параметрлердің сапалық бағалауларын сипаттайтын сандық эквиваленттер жиынының бейнесіне сәйкес келеді.

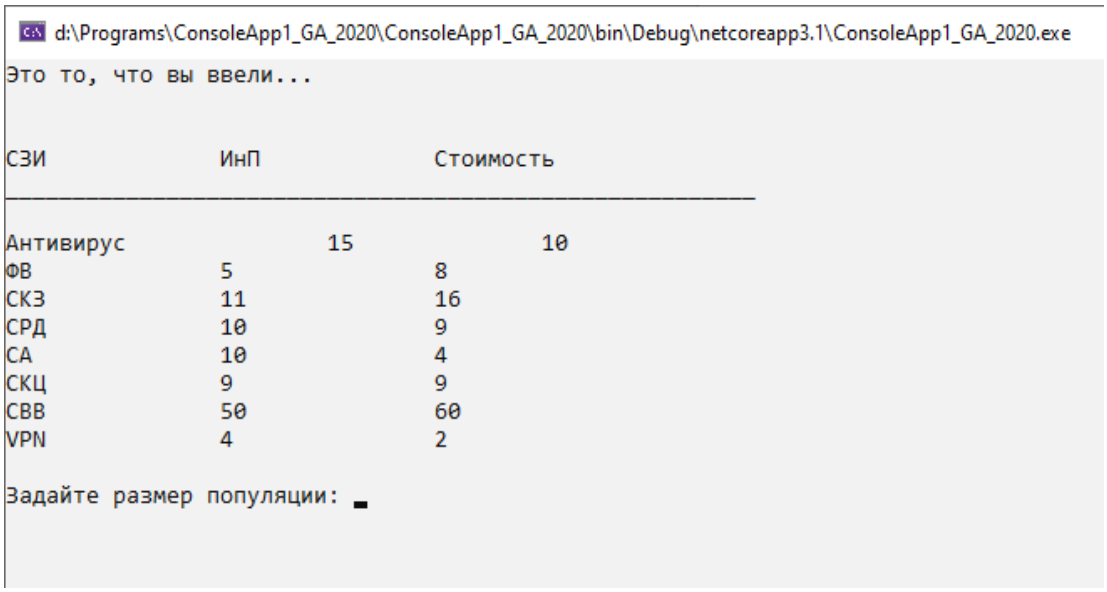
Рюкзак есебін шешу үшін классикалық ГА пайдалану жағдайында қарапайым кроссинговер мен мутация операторларын қолданумен байланысты есеп туындауы мүмкін екенін ескереміз. Егер бір нүктелі кроссинговер операторын қолданса, онда таңдалған ата-аналық хромосомалардан қате шешімді кодтайтын ұрпақ пайда болуы мүмкін. Шын мәнінде, логикалық вектор АКЖ түйініндегі АҚҚ жиынтығын сипаттайтын жағдайға тап болу мүмкін, ол үшін интегралдық көрсеткіш берілген деңгейден бірнеше есе асады.

Сол сияқты, тұрақты мутация операторын қолдану хромосоманың пайда болуына әкелуі мүмкін, ол тапсырма үшін жарамсыз шешімді кодтайды.

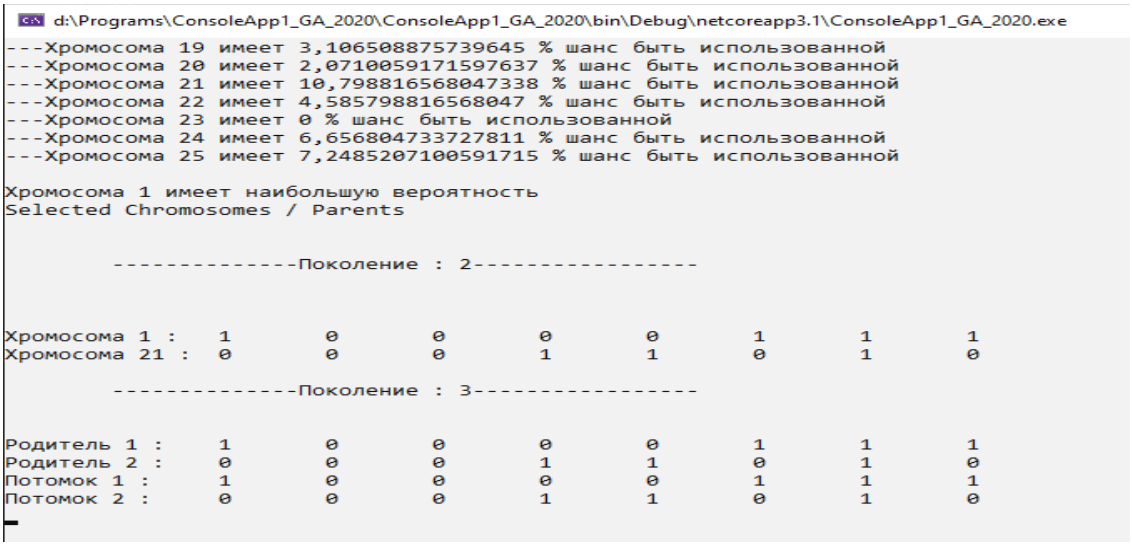
Егер алынған хромосомаларды түзету қолданылса, жоғарыда аталған қиындықтарды болдырмауға болады. Түзету келесі процедураны жүзеге асырудан тұрады. Алынған хромосомада биттердің жарамсыз кодталуы бар, кездейсоқ жеке гендерді таңдаймыз. Бұл таңдалған (1) гендер рұқсат етілген хромосома алынғанша нөлдік (0) гендерге ауыстырылады.

Сол сияқты мутация нәтижесінде алынған хромосомаларға түзету жүргіземіз. АКЖ түйіндері бойынша АҚҚ іріктеу процесінде ГА қолдануға арналған консоль қосымшасының интерфейсі төменде келтірілген.

3.2-суретте бастапқы деректері бар қосымшаның терезесі, ал 3.3-суретте модельдеу нәтижелері бар терезе көрсетілген. Қорғаныс құралдарының элементтерінің немесе кластарының саны 8-ге тең, яғни NIST ұсынған барлық қорғаныс кластары үшін хромосомаларды іріктеу жағдайы модельденеді. Ұсыныстарға сәйкес, NIST [13, б.7, 14, б. 10] түйіндерде АҚҚ-ның барлық кластары орналасуы керек, 3.1-суретті қараңыз: вирусқа қарсы БҚ (Антивирус); құралдары - файервол (ФВ); криптографиялық қорғау (КҚ), қолжетімділікті шектеу (ҚЖШ), аутентификация (АҚ), тұтастығын бақылау (ТБҚ), басып кіруді анықтау (БАҚ) құралдары; VPN (VPN). Бағдарламаның листингі А қосымшасында келтірілген.



3.2-сурет – ГА көмегімен АКЖ түйіні үшін АҚҚ таңдауға арналған бастапқы деректер тізбесі бар терезе



3.3-сурет – ГА көмегімен АКЖ түйіні үшін АҚҚ іріктеуді ұтымды шешу процесін модельдеу нәтижелері бар терезе

ГА жұмысы келесі жағдайларда аяқталады: 1) икемделу-функцияның мәндері неғұрлым бейімделген особьтарға және бірнеше жүйелі популяцияларда сәйкес келеді; 2) ұрпақтардың алдын ала келісілген санына қол жеткізілгенде. ГА-ның тағы бір кемшілігі - қажетті шешім икемделу функциясының жергілікті максимумына сәйкес келетін, бірақ сонымен бірге локальді максимумға сәйкес келмейтін кезде оның жұмысын мерзімінен бұрын аяқтауы мүмкін. Диссертацияның екінші тарауында көрсетілгендей, бұтақтар мен шекаралар әдісіне (БШӘ) негізделген алгоритмдерде бұл кемшілік жоқ. Алдыңғы бөлімдерде айтылғандай, бұтақтар мен шекаралар әдісі экспоненциалды күрделілікке ие және үлкен өлшемді тапсырмаларда қолдану мүмкіндігі шектеулі болса да, ол іздеу процедурасына үлкен дәлдік бере отырып, ГА-ны толықтыра алады [84].

Жоғарыда айтылғандарды ескере отырып, қорғау тарапының ресурстарын іріктеу, ұтымды шешу және қайта бөлу есебін шешу үшін ГА модификациясы болып табылатын және БШӘ элементтерімен толықтырылған құрамдас алгоритмді (немесе түрлендірілген алгоритмді) қолдану ұсынылады.

Құрама әдісті қолданудың мәні бірінші кезеңде есепті шешу үшін ГА қатысады. Екінші кезеңде ГА көмегімен табылған шешімді БШӘ есебінен жақсартуға болады.

ГА көмегімен түйінде (рюкзакта) АҚҚ жиынтығын қалыптастыру мүмкіндігі табылды. Жинақ бірден ұтымды бола бермейді. Бірақ ГА арқылы алынған кез-келген шешім сияқты, жиынтықтың табылған нұсқасы $(ch_1, ch_2, ..., ch_k)$ хромосома түрінде кодталады, ол 1 және 0-ден тұрады, онда k – түйіндегі ЖҚҚ заттарының саны, 3.1суретті қараңыз.

Әрбір торапта орналасқан ақпаратты қорғау құралдары олардың ИнК кему тәртібімен нөмірленеді. Мысалы, қол жеткізуді бөлу құралдары VPN-ге қарағанда жоғары орналасқан. Егер хромосомада бит 1-ге сәйкес келсе, онда тиісті АҚҚ АКЖ түйінінде орналасқан деп санаймыз, егер 0 болса, онда болмайды.

Іс жүзінде «сараң алгоритм» жиі қолданылады, оған сәйкес ең құндыны рюкзактарға салу керек. Соңғы *h*- элементтерді $(ch_1, ch_2, ..., ch_k)$ жолдан алып тастаймыз. Нәтижесінде $(ch_1, ch_2, ..., ch_{k-h})$ жолды аламыз. Бұл жол АКЖ түйінін (рюкзакты) толтыру нұсқасына сәйкес келеді, онда түйінді толтырған және $n-h$ үлкен нөмірлері бар барлық заттар рюкзактан шығарылады.

Содан кейін $(ch_1, ch_2, ..., ch_{n-h})$ жолды h санмен биттермен (гендермен) толықтыруға болады. Нәтижесінде түйінді толтырудың жаңа нұсқасын аламыз. Бұл жаңа нұсқада ГА-мен табылған шешіммен салыстырғанда түйін (рюкзак) үшін жоғары ИнК бар.

Сонымен қатар, ШБӘ қолдана отырып, $(ch_1, ch_2, ..., ch_{n-h})$ жолды жалғастырудың ең жақсы нұсқасын таба аласыз. Шынында да, $(ch_1, ch_2, ..., ch_{k-h})$ жолда АКЖ түйінінде жиналған АҚҚ бар. Бұл түйіннің бос бөлігінің сыйымдылығы түйінге (рюкзакқа) орналастырылған заттардың ИнК мөлшеріне сәйкес азайғанын білдіреді. Демек, IND' ИнК (сыйымдылығы) және C' құны бар жаңа рюкзак бар деп санаймыз, мұнда

$$IND' = IND - \sum_{i=1}^{k-h} a_i \cdot ch_i, \tag{3.3}$$

$$C' = \sum_{i=1}^{k-h} c_i \cdot ch_i, \tag{3.4}$$

мұнда IND – АҚҚ интегралдық көрсеткіші.

Осылайша, ГА көмегімен АКЖ түйініне (рюкзакқа) АҚҚ іріктеу кезеңін іске асырғаннан кейін, тапсырманы аз көлемді рюкзакқа қойдық, оны аз заттармен толтыру қажет.

Енді ШБӘ қолдануға болады. Біз h биіктігі бар екілік ағаш саламыз. Әр шыңға 1 және 0-ден тұратын k ұзындық сызығы сәйкес келеді.

Жолдағы бірліктер түйінде орналасқан АҚҚ нөмірлерін көрсетеді. Екілік ағаштың тамыры h биіктікке ие. Түбірге $(ch_1, ch_2, ..., ch_{k-h}, 0, ..., 0)$ жолы сәйкес келеді. k биіктіктің шыңына $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 0, ..., 0)$ жолы сәйкес келеді. Сонда $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 1, 0, ..., 0)$ және $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 0, 0, ..., 0)$ жолдар тікелей ұрпақтарға сәйкес келеді және мұнда $l = 2,3,..., h$.

Ұрпақ жолдары АҚҚ түйінін толтырудың «жақын» нұсқаларын кодтайды. Ұрпақтар бір-бірінен ерекшеленеді, өйткені бірінші жағдайда түйінде $n-h$ нөмірі бар зат (АҚҚ) болады, ал екіншісінде болмайды.

Барлық жолдар рұқсат етілмейді деп ойлаймыз, яғни максималды ИнК ескере отырып, түйінді толтырудың рұқсат етілген нұсқасын сипаттай алады. Сондықтан жарамсыз сызықтарға сәйкес келетін шыңдарда ұрпақтар болмайды.

k биіктігі бар шыңға $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 0, ..., 0)$ рұқсат етілген жол сәйкес келеді деп болжаймыз, мұнда $l = 2,3,..., h$ осы шыңға PS перспективасы сияқты параметрді есептейміз.

Бинарлық ағаштың шыңдарының перспективасы деп АОБ қорғау тарабының шектеулі ресурстары жағдайында АКЖ торабындағы АҚҚ жиынтық құнына салынған шектеу мөлшерін болжайтын боламыз. Шын мәнінде, параметр PS – бұл АКЖ түйінінде орналасқан АҚҚ-ның максималды құны, егер оның $1,2,3,..., k-l$ нөмірі бар заттар түйінде орналасқандығы белгілі болса, анықтауға болады. PS параметрін келесідей есептеледі:

$$\begin{aligned} PS = & \sum_{i=1}^{k-h} c_i \cdot ch_1 + \sum_{j=1}^{h-l} c_{k-h+j} \cdot z_j + \\ & + \left(IND - \sum_{i=1}^{k-l} a_i \cdot ch_1 - \sum_{j=1}^{h-l} a_{k-h+j} \cdot z_j \right) \cdot \frac{c_{k-l+1}}{a_{k-l+1}} \end{aligned} \tag{3.5}$$

Сонда екілік ағаштың шыңының бірінші деңгейі үшін PS параметрді келесідей есептейміз:

$$PS = \sum_{i=1}^{k-h} c_i \cdot ch_1 + \sum_{j=1}^{h-1} c_{k-h+j} \cdot z_j + c_k. \tag{3.6}$$

ШБӘ-ға сәйкес екілік ағаш жоғарыдан төменге қарай салынған. Құрылыстың әр кезеңінде келесі шың *PS* параметрді есептеу нәтижелеріне негізделген. Көрнекі мысал үшін біз антивирустық БҚ мен брандмауэр артық деп сеніп, тапсырманы сәл жеңілдетеміз. Windows 10 ОЖ соңғы нұсқасында антивирус әдепкідей орнатылады және оның жоғары рейтингтері қымбат коммерциялық антивирустық бағдарламаны пайдаланбауға мүмкіндік береді. Бұл брандмауэрге де қатысты. Сондықтан, иллюстрациялық мысалда біз тек 6 затты қалдырамыз: құралдар - криптографиялық қорғау (ККҚ), қол жетімділікті шектеу (ҚЖШ), аутентификация (АҚ), тұтастықты бақылау (ТБҚ), басып кіруді анықтау (БКАҚ); VPN. Содан кейін АКЖ түйініне арналған бастапқы мәліметтері бар кесте келесідей көрінуі мүмкін, 3.1-кестені қараңыз. Мысалдағы АҚҚ құны ұлттық валюталарға байланысты болмас үшін шартты бірліктерде немесе баллдарда көрсетілген. АҚҚ-ның интегралдық көрсеткіштері балдық бағалау негізінде, мысалы, www.anti-malware.ru сайты [85] деректері негізінде, сондай-ақ сараптамалық бағалау және өрнектің қолданылуын ескере отырып қабылданды (3.2).

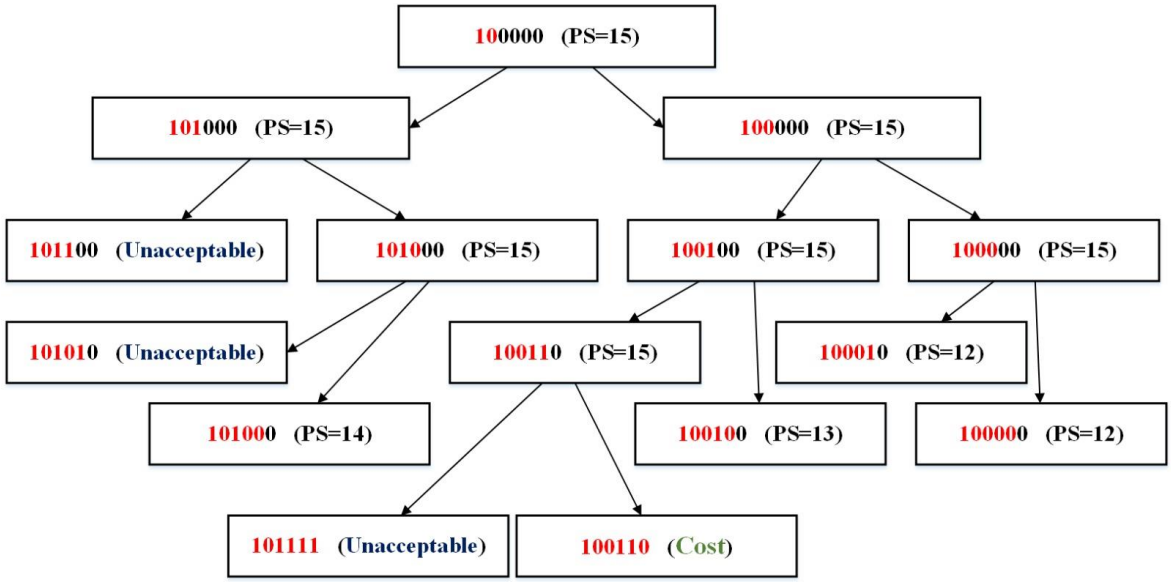
3.1-кесте – АКЖ түйіні үшін ұтымды шешу есебін шешуге арналған бастапқы деректер

Пән нөмірі	1	2	3	4	5	6
АҚҚ атауы	ККҚ	ҚШЖ	АҚ	ТБҚ	БККҚ	VPN
Шартты бірліктердегі құны	5.0	7.0	8.0	6.0	4.0	1.0
Интегралдық көрсеткіш (ИнК)	2	3	4	3	2	1

ГА жұмысының нәтижесінде АКЖ АҚҚ түйінін ораудың белгілі бір нұсқасы анықталды делік. Нәтиже $ch = 101001$ хромосомаға жазылады. Біз ИнК тестінің мысалына 7-ге тең қоямыз (іс жүзінде бәрі таңдалған ИнК бағалау шкаласына байланысты. Мысалы, ол 1-ден 10-ға дейін немесе 1-ден 100-ге дейін өзгеруі мүмкін).

$IND = 7$ көрсеткіш үшін жиынтық ИнК 7-ге тең болады, ал түйіннің АҚҚ құны – 14 ш.б.

$h = 4$ параметр болсын. Содан кейін параметр жоғарыда сипатталған өзгертілген алгоритмді (ГА+ ШБӘ) қолдана отырып, 3.4-суретте көрсетілген екілік ағашты (ЕА) аламыз.



3.4-сурет – ГА мен ШБӘ-ны біріктірген түрлендірілген алгоритм жұмысының иллюстрациясы

Біз екілік ағашты жоғарыдан бастаймыз, ол 100000 жолға сәйкес келеді. Жол 4 биіктікте орналасқан. Бұл жолдың параметрі PS =15 тең. Бұл - түйіндегі барлық АҚҚ-ның ИнК қосындысына тең түйіндегі максималды ИнК.

Соңғы h элементтерді (101001) жолдан алып тастаймыз. Нәтижесінде (100000) жолды аламыз . Бұл жол АКЖ түйінін толтыру нұсқасына сәйкес келеді, онда түйінді толтырған және $k-h$ үлкен нөмірлері бар барлық заттар рюкзактардан шығарылады. 3.4-суретте рюкзакқа (түйінге) кірген АҚҚ кодтайтын жолдың сол жағындағы сақталған биттер қызыл түспен көрсетілген.

Әрі қарай, екілік ағаштың келесі деңгейінде (100000) жолды . көлемінде биттермен (гендермен) толықтырамыз. Содан кейін 3-ш биіктіктегі ұрпақтардың жолдары келесідей болады: (101000) және (100000) . Ұрпақтың деректер параметрлері де PS =15 болып табылады.

Біз Екілік ағашты (101000) шыңнан салуды жалғастырамыз. Келесі екі ұрпақ қалыптасады, сәйкесінше – (101100) және (101000) жолдарымен ұсынылған. Бірінші ұрпақ, яғни (101100) жол рұқсат етілмейді, өйткені түйіндегі АҚҚ-ның жиынтық құны рұқсат етілген шекарадан асады (БҚҚ(5.0)+СВВ (8.0)+ТБҚ(6.0)=19.0 ш.б.). Екінші ұрпақ, яғни PS =15 жол болуы мүмкін, сонымен қатар, екі ұрпақты береді, сәйкесінше жолдар – (101010) және (101000). Сонымен қатар, егер бірінші жол ұрпағына жол берілмесе (КҚҚ (5.0)+ АҚ(8.0)+БҚҚ (4.0)=17 ш.б.), онда екінші жол рұқсат етіледі, бірақ ол PS =15 берілген мәннен аз, сондықтан Екілік ағаштыңбұл бөлігін бұдан әрі құрудың мәні жоқ.

Екілік ағаштың жоғарғы жағына өтейік, ол (100000) жолда жазылған. Онікі PS =15 . Жоғарыда сипатталғандай ойлана келе, (100000) жолдың ұрпақтарын талдаймыз. Бұл жол ұрпақтардың жолдарын құрайды -(100100) және (100000) . Олардың параметрі - PS =15. Тиісінше әрбір жол ұрпақтары өз ұрпақтарын

береді. Ұрпақтардың әр -(100100) жолы да сәйкесінше -(100110) және -(100100) ұрпақтарын береді.. Ал (100000) жол (100010) және (100000) ұрпақтарды береді. Алайда (101100), (101010) және (101111) шыңдарында АҚ көмегімен АКЖ түйінін орау нұсқасына сәйкес келмейтін биттер болады.

Егер түйінде 1 зат (КШЖ) орналасса ал 2 зат (ККҚ) болмаса онда (100110) жолы шартты түрде ең жақсы деп есептеледі. Осылайша, ГА артықшылықтары мен бұтақтар мен шекаралар әдісін біріктіретін өзгертілген алгоритмді қолдана отырып, тек ГА арқылы алынған шешімді жақсартуға болады.

Бұл жағдайда модификацияланған (құрама) алгоритм АКЖ түйіндерінің (рюкзактарының) саны едәуір үлкен болған жағдайда қызықты және классикалық әдістермен олардағы барлық ресурстарды қайта бөлуді ұтымды шешу есебін қатар шешу өте қиын процесс.

Өзгертілген алгоритмнің жұмыс уақыты популяция мөлшері мен ұрпақтар санына тікелей пропорционалды, ал жиынтықтағы заттардың k санына көпмүшелік санға байланысты болады. Өзгертілген алгоритмнің жұмыс уақыты көбінесе h параметрдің көлеміне байланысты болады.

Жоғарыда сипатталған сынақ мысалына және 3.2 және 3.4-суреттерінде көрсетілген нәтижелерге ұқсас, k және h бөлшек мәндер үшін есептеу эксперименттері жүргізілді.

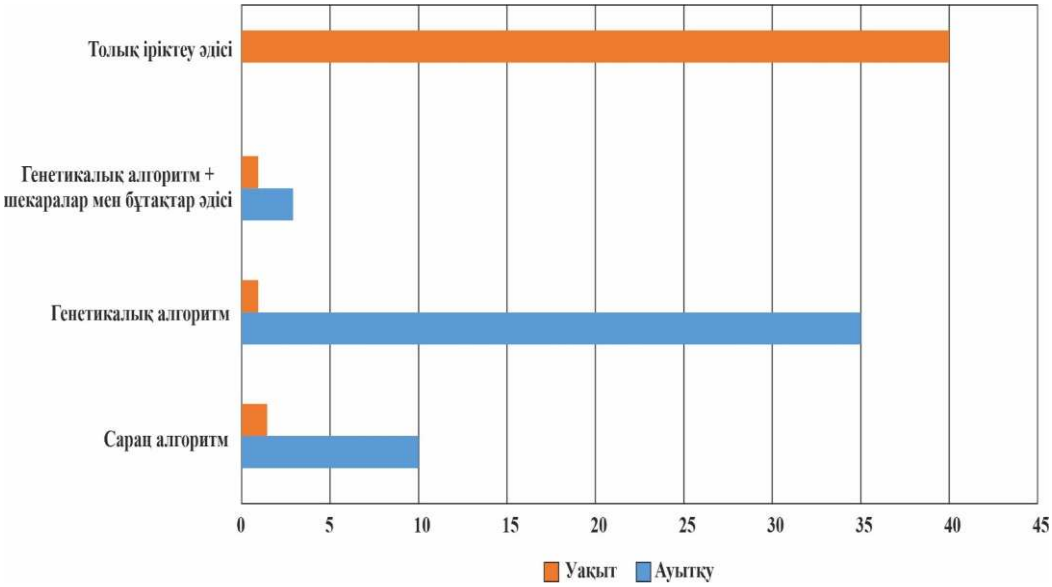
Ұсынылған модификацияланған құрама алгоритмді (ГА+ШБӘ) ұқсас есептер класын шешу үшін қолданылатын басқа классикалық алгоритмдермен салыстыру үшін классикалық ГА, «сараң» (СА) және нақты толық санау (ТС) алгоритмімен салыстырмалы талдау жасалды.

Жоғарыда аталған алгоритмдерді бағалау үшін жиынтықта 5-тен 150-ге дейін тақырып жиынтығы (АҚҚ) жасалды. Серияда 30 тәжірибе бойынша 5 серия өткізілді, 3.2-кестені қараңыз. Барлығы 150 есептеу тәжірибесі. Есептеу эксперименттері Inteli7 9750h (2.6 – 4.5 ГГц) процессоры бар компьютерде жасалды.

Жұмыстың екінші тарауында көрсетілгендей, АКЖ түйіндеріндегі ақпаратты қорғау контурларының аппараттық-бағдарламалық компонентіне ғана емес, сонымен қатар ұйымдастырушылық шараларға да назар аудару маңызды болғандықтан, АКЖ-ны қорғау дәрежесін жоғарылату үшін жұмыс тізіміндегі заттар тест жинақтарына да енгізілді. Бұл жұмыстар да құны мен интегралды индикатормен сипатталуы мүмкін.

3.5-суретте және 3.2-кестеде алгоритмдердің салыстырмалы сынақтарының нәтижелері көрсетілген. 3.1-кестеде көрсетілген заттар тізбесіне қосымша: телефон желілерін қорғау құралдары; үй-жайларды виброакустикалық қорғау жүйелері; сөйлесуге арналған үй-жайларда кедергілер қою құралдары; түрлі арналар бойынша ақпараттың тарауын анықтау құралдары; бейнебақылау құралдары және т. б. енгізілді [86].

Толық сұрыптаудың дәл әдісін қолдана отырып алынған шешімдер дәлірек болды деп күтілуде. Бірақ мұндай алгоритмнің жұмыс уақыты, тіпті i7 процессорларын қолдануды ескере отырып, ГА немесе ГА+ШБӘ-ға қарағанда 17-25 есе көп.



3.5-сурет – Әртүрлі алгоритмдер үшін нақты шешімдерден орташа ауытқулар және шешім табу уақыты

ГА мен ШБӘ-ты біріктіретін модификацияланған алгоритм диссертацияның келесі бөлімдерінде толығырақ сипатталатын әзірленген бағдарламалық өнімнің есептеу ядросына кіреді.

3.2-кесте – Пәндер жиынтығын – АКЖ түйіндеріне арналған ақпаратты қорғау құралдарын қалыптастырудың әртүрлі алгоритмдеріне арналған салыстырмалы тест нәтижелері (нақты нәтижеден берілген ауытқу үшін 2,8% артық емес)

№ сериядағы тәжірибе	Тест жиынтығындағы заттар саны - N	Алгоритмдер			
		Толық санау	Классикалық ГА (популяция мөлшері 50)	«Сараң» алгоритм	ГА+ ШБӘ (популяция мөлшері 50)
		Шешім уақыты, с			
1	5	1	1	1	1
2	10	1	1	1	1
3	15	600	1	1	1
4	20	720	1	1	1
5	35	1000	1	1	1
6	30	1300	1	1	1
7	35	1600	1	1	1
8	40	2200	1	1	1
9	45	4500	1	1	1
10	50	4900	1	1	1
11	55	6020	1	1	1
12	60	7990	1	1	1
13	65	8900	1	1	1
14	70	9400	1	1	1
15	75	10100	1	1	1
16	80	10690	1	1	1
17	85	11450	1	1	1
18	90	11990	1	1	1
19	95	12670	1	2	2
20	100	13300	1	2	2
21	105	13900	1	2	2
22	110	14200	1	3	2
23	115	14800	1	3	2
24	120	15220	2	4	3
25	125	15700	1	4	3
26	130	16300	3	5	4
27	135	16500	3	6	4
28	140	16900	3	7	5
29	145	17500	4	8	5
30	150	18000	5	10	6

3.2. Ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасын, қорғау құралдарының интегралдық көрсеткіштерін және олардың құнын пайдалануды ескере отырып, генетикалық алгоритмді дамыту

Тапсырманы ГА тұрғысынан ресімдейміз. Хромосома қорғаныс шараларының жиынтығы деп санаймыз (мысалы, қорғаныс объектісінде ақпараттық қауіпсіздік саясатын сақтау ережелері), соның ішінде АҚҚ. Жиын екілік сан түрінде кодталған. Егер санның екілік разряды (1) бірлікке тең болса, онда тиісті АҚҚ немесе тиісті нөмірі бар ақпаратты қорғау жөніндегі шара жиынтыққа енгізіледі. Содан кейін кодты өзгерту ауқымын келесідей ұсынуға болады:

$$G = (d_0 d_1 ... d_{NC})_2 = (0...2NC)_{10}, \quad (3.7)$$

мұнда NC – ұтымды жиынтыққа қосу үшін ықтимал қарастырылатын АҚҚ және қорғау шараларының саны; d_i – АҚҚ және/немесе қорғау шараларын жиынтыққа қосу.

ГА терминдерінде популяция әртүрлі хромосомалары бар үлгілерден тұрады. Популяция мөлшері ондағы үлгілердің максималды санымен шектеледі. Популяцияның әр данасын келесідей сипаттауға болады:

$$Ch = \{G, C, R\}, \quad (3.8)$$

мұнда G – популяциядағы генетикалық коды экземпляры;

C – АҚҚ және/немесе тиісті қорғау шараларының құны;

R – таңдап алынған АҚҚ және/немесе 2-тарауда (бұдан әрі қабылданған АҚҚ) қаралған тиісті қорғау шараларын ескере отырып, ақпаратты (немесе оның құпиялылығын, тұтастығын) жоғалтудың жиынтық тәуекелі.

Тәуекелді анықтау үшін алгоритмді өзгерту процесінде келесі болжам қолданылады. Белгілі бір АКЖ үшін ақша эквивалентіндегі шығындардың абсолютті мәні элементтер -қауіптер, осалдықтар, АҚҚ тізбегіне байланысты. Сондықтан тәуекелдер саны - бұл қауіптер мен активтердің жиынтығы:

$$R = TH \cdot M, \quad (3.9)$$

мұнда TH – қауіптер саны, M – активтер саны.

(3.9) формуласында бірнеше қауіптердің үйлесуі, сондай-ақ АҚҚ арасындағы ішкі әсер ескерілмеген. Сондықтан АКЖ үшін қауіптерді анықтаудың неғұрлым қолайлы әдісі шабуыл профильдерін жасауға негізделген әдіс болып табылады [86, 165-б]. Бұл әдіспен шабуыл профильдері әртүрлі қауіптердің үйлесімінен тұратын шабуылдар тізбегі ретінде қарастырылады. Сонда тәуекелдер санын келесі тәуелділікпен сипаттауға болады:

$$R = \left(2^{TH}\right)^{TA} \quad (3.10)$$

мұнда TA – шабуылдар саны.

Демек, берілген профиль үшін тәуекелдің шамасы сәтті шабуылдардан келтірілген жалпы залалдың мөлшері деп санауға болады.

Егер шабуыл кезінде тізбекті реакция болмаса, онда жалпы тәуекелдің мәні әрбір АКЖ активі үшін зиянды математикалық күту ретінде ұсынылуы мүмкін:

$$r = \sum P_{i,j} \cdot D_{i,j}, \quad i = \overline{1,TH},\ j = \overline{1,M}, \quad (3.11)$$

мұнда $P_{i,j}$ – (j) активке (i) қауіп төндіретін АКЖ ақпараттық қауіпсіздік қақтығысының ықтималдығы;

$D_{i,j}$ – оқыс оқиғаға байланысты залалдың мөлшері (ақшалай баламада қабылданған).

(Ch) хромосома матрица түрінде ұсынылуы мүмкін. Содан кейін матрицаның жолдары орналастыру нүктелері болады, сәйкесінше бағандар –

нақты АҚҚ-ны қамтитын құралдар класы (мысалы, антивирустық БҚ класы қарастырылған антивирустық бағдарламалардың барлық нұсқаларын қамтуы мүмкін: Avast, Avira, AVG, Bitdefender және т.б.). g_{ij} матрица элементі *i* түйінге орналастырылған *j* кластан ақпаратты қорғау құралының нөмірін көрсетеді. Егер $g_{ij} = 0$, онда *j* кластан *i* түйінде бірде-бір құрал пайдаланылмайды деп есептейміз, мысалы, вирусқа қарсы БҚ желіаралық экранда пайдаланылмайды.

ГА (Ch) хромосомасының қалыптасу схемасы 3.3-кестеде келтірілген.

3.3-кесте. Хромосоманың қалыптасу схемасы

Қарсы шаралар кластары. Желі тораптары	N_1	N_2	…	N_{NC}
K_1	g_{11}	g_{12}	…	g_{1NC}
K_2	g_{21}	g_{22}	…	g_{2NC}
…	…	…	…	…
K_{KC}	g_{KC1}	g_{KC2}	…	$g_{KC,NC}$

Мұндай форматта ұсыну хромосоманың және контекстінде шешілетін есептер деп K_{KC} және N_{NC} – тиісінше, түйіндеріндегі АКЖ және АҚҚ түйіндерінің саны. (R) тәуекелді есептеу үшін келесі модельді қолданамыз. Генетикалық код бойынша әрбір тасымалдаушы үшін тиісті АҚҚ-ны таңдаймыз.

ГА-ға $U-.$ пайдалылық функциясын енгіземіз: бұл функция жиынтықта таңдалған АҚҚ тиімділігін бағалау үшін қажет. Таңдалған АҚҚ шабуыл профиліне сәйкес келуі керек екенін ескертеміз. Өйткені, мысалы, шектеулі функционалдығы бар тегін антивирустық бағдарламалық қамтамасыз ету (БҚ) DoD/DDoS шабуылдарымен күресу үшін мүлдем пайдасыз екендігі түсінікті, ал АКЖ-ге арналған қауіпсіздік саясатын сақтау жөніндегі нұсқаулар инсайдерлерден қорғамайды.

Онда $U-.$ пайдалылық функцияны келесідей беруге болады:

$$U(Ch) = R_0 - Ch.R, \tag{3.12}$$

мұнда Ch – АҚҚ жиынтығының данасы;

R_0 – егер АҚҚ-ның тиісті жиынтығын қолданбаса, ақпараттың жоғалуына байланысты тәуекелдердің шамасы;

$Ch.R$ – АҚҚ-ның тиісті жиынтығын *Ch.G.* (данасын) қолдануды ескере отырып, тәуекелдер шамасы

Алайда, АКЖ-ны шабуылдардан қорғау бойынша қол жеткізілген ұтымдылық, тиісінше, АҚҚ-ға қосымша шығындарды талап етеді. Келесі қатынасты қолдана отырып, АҚҚ-ға шығындардың әсерін ескереміз:

$$U(Ch) = {(R_0 - Ch.R)}/{Ch.C}, \tag{3.13}$$

мұнда $Ch.C$ – АҚҚ жинағының құны.

(3.13) формула қатынас әрбір салынған құн бірлігіне ақпараттың жоғалу қаупін қалай азайтуға (немесе арттыруға) болатындығын көрсетеді.

Әрі қарай, біз алынған өрнектерді ГА-да қалай қолдануға болатынын қарастырамыз. Жоғары деңгейлі бағдарламалау тілдерінің синтаксисінде кроссинговер, мутация, таңдау функциялары келесідей болады.

Кроссинговердің функциясы - жаңа тасымалдаушылардың өнімі. ГА базасында ШҚҚЖ бағдарламалық іске асыру процесінде кроссинговердің екі түрі қаралды. Бір нүктелі және n-нүктелі кроссинговерді қолдану мүмкіндіктері талданды. Осы екі түрді таңдау келесі ойларға байланысты. Бір нүктелі кроссинговерге негізделген стандартты тәсіл ГА көмегімен шешім табуға болатын көптеген тапсырмаларға сәйкес келеді, алайда АКЖ түйіндеріне арналған АҚҚ көп таңдау есептері үшін стандартты ГА өте дәл болмайды. Бұл хромосома біртұтас бөлінбейтін құрылым болмайтындығына байланысты. Бұл есепті шешуде хромосоманы ыдырау процедурасын қажет ететін жүйе ретінде түсіндіруге болады. Декомпозиция хромосоманы бөліктерге бөлуге мүмкіндік береді және әр бөлім АКЖ түйіндерінің өзіндік класына сәйкес келеді.

Біз әр жұп үшін (PA) ата-аналардың ерекшеліктерін мұра ететін жаңа дана жасаймыз.

$$\begin{aligned} &func\ K(PA) := foreach\ Ch(X)\ from\ PA\ and \\ &foreach\ Ch(Y)\ from\ PA\ where\ Ch(X) != \\ &Ch(Y)\ do\ R.add(\{G : xor(Ch(Xi).G, Ch(Xj).G),\ C :,\ R :\}) \\ &return\ R.add(PA) \end{aligned} \tag{3.14}$$

Әрі қарай, мутация функциясын, яғни генетикалық кодтың өзгеруін қарастырыңыз. Мутацияның екі түрі қарастырылды. Бұл келесі болжамдарға байланысты:

1) тұрақты мутация ГА бағдарламалық жасақтамасының көпшілігінде қолданылады;

2) біздің есебіміздің айнымалылары икемділікті қажет етеді және біздің есеп үшін ГА-ның сәтті жұмысының мутацияға тәуелділігі кроссинговерге қарағанда көбірек;

3) 2-болжам АКЖ КҚ контурларын қалыптастыруға байланысты есептерді шешудің объективті ерекшеліктері бар екендігіне байланысты. Бұл хромосомалардың үлкен мөлшеріне, сондай-ақ шектеулердің болуына әкелді.

Сондықтан, кездейсоқ элементтермен сипатталатын ауыспалы мутация, алгоритмнің алғашқы кезеңдеріндегі рюкзактың ұтымды құрамын табу тұрғысынан қолайлы болады.

Есептеу эксперименттері барысында мутацияның екі түрі қарастырылды. Бірінші түрі - тұрақты мутация. Бұл жағдайда 1% ықтималдығы бар хромосомадағы әр позиция инверттеледі. Екіншісі -ауыспалы мутация. Бұл жағдайда мутация ықтималдығы ГА-ның қазіргі қажеттіліктеріне байланысты болады. Мутация коэффициенті 1-6% аралығында болады.

Салыстырмалы икемделу функциясы бар қарастырылып отырған ГА-да

икемделу функциясы ретінде хромосома құрайтын АҚҚ тиімділігінің қосындысы емес, класқа кіретін АҚҚ-ның тиімділігі немесе интегралдық көрсеткіштерінің қосындысы қолданылды.

Ол үшін хромосомадағы екі екілік разрядты кездейсоқ түрлендіреміз:

$$\begin{aligned} &func\ M(PA) := foreach\ Ch(X)\ from\ PA\ do\ Ch(X).G = \\ &= xor(Ch(X).G, 1 << rand(0, NC)). \end{aligned} \tag{3.15}$$

Онда таңдау функциясы, яғни ең жақсы тасымалдаушыны таңдау келесідей ұсынылуы мүмкін:

$$func\ S(PA) := return\ PA.sort(\ ).slice(1, K). \tag{3.16}$$

Жазбаны азайту және популяцияны азайту үшін тек (U) пайдалы функцияға қатысты үлкен нәтиже беретін K тасымалдаушыларды қалдыратынымызды ескертеміз.

Таңдауды қолданар алдында популяция үшін $Ch(X).C$ және $Ch(X).R$ алдын-ала есептейміз. [86, б.67-72] сәйкес бастапқы популяция кем дегенде екі үлгіні қамтиды деп қабылданды. Сонда ГА-дағы әр дәуір жоғарыда қарастырылған негізгі функцияларды дәйекті қолданудан тұрады. Тиісінше, мынаны аламыз:

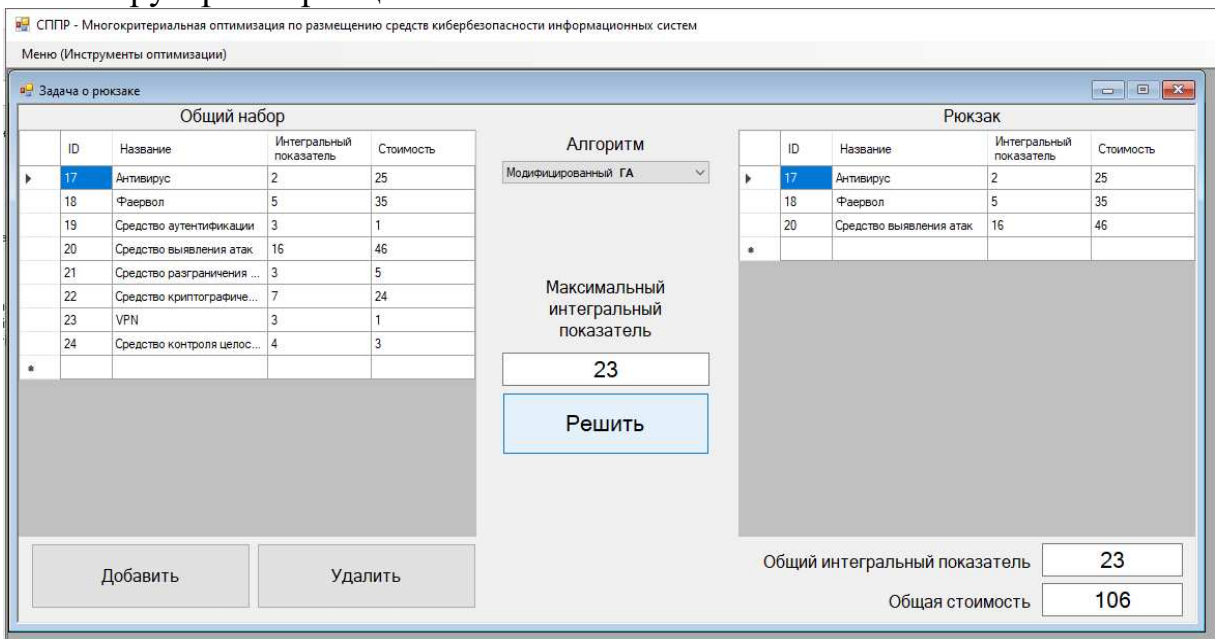
$$func\ E(\ ) := ((PA = K(PA), M(PA)), (P = S(PA))). \tag{3.17}$$

ШҚҚЖ жұмысының нәтижесінде тиісті кластан әрбір АҚҚ-ның интегралдық көрсеткіші және осы АҚҚ-ның құны негізінде АКЖ түйіні үшін АҚҚ-ның ұтымды жиынтығы айқындалады. АҚҚ кластары үшін ИнК талдау және есептеу негізінде оларды қалыптастырудың сараптамалық әдісін қолданбай АҚҚ кластары үшін салмақтық коэффициенттерге негізделген ИнК максималды мәні туралы түсінік жасауға болады. ШҚҚЖ есептеу ядросының бағдарламалық жасақтамасы, жоғарыда сипатталған модельдер, сонымен қатар Microsoft Visual Studio 2019 ортасында c# тілінде орындалған АКЖ КҚ контурлары үшін АҚҚ жиынтығын құрудың ұтымды стратегиясын табу есебін жүзеге асыратын алгоритм жұмыстың келесі тарауында толығырақ сипатталады. Сондай-ақ, оның нақты АОБ-дегі тестілеу нәтижелері көрсетілген.

ШҚҚЖ тұжырымдамасы АКЖ-ның қол жетімді архитектурасы, кластар мен АҚҚ жиынтығы негізінде, сондай-ақ бірінші кезеңде иерархияларды талдау әдісін (Т.Саати әдісі) қолдана отырып, ГА+ШБӘ көмегімен АКЖ-ның негізгі түйіндерінің әрқайсысында АҚҚ-ны орналастырудың ұтымды нұсқасын қалыптастыру есебі шешіледі, 3.1-суретті қараңыз. ШҚҚЖ негізгі терезесі 3.6-суретте көрсетілген.

Кибернетикалық қауіпсіздіктің қажетті деңгейін қамтамасыз ету және есептеу параметрлерін реттеу үшін АКЖ түйінінде қолданылуы мүмкін КҚ және АҚ (яғни хромосомалар) қамтамасыз етуге арналған заттардың жалпы жиынтығына қатысты барлық деректерді енгізгеннен кейін тікелей ГА басталады. Сол үшін ГА 25 хромосомадан тұратын популяцияны құрайды. Әрі қарай, әр хромосоманың икемделу функциясы (тиімділігі) есептеледі. ГА-да k-

нүктелі кроссинговер қолданылған. Шын мәнінде, k – АКЖ-ғаарналған АҚҚ орналастыру нүктелерінің саны.



3.6-сурет – ШҚҚЖ модулі интерфейсінің жалпы түрі (модуль-түйін үшін АҚҚ құрамын таңдау есебін шешу үшін ГА қолдану)

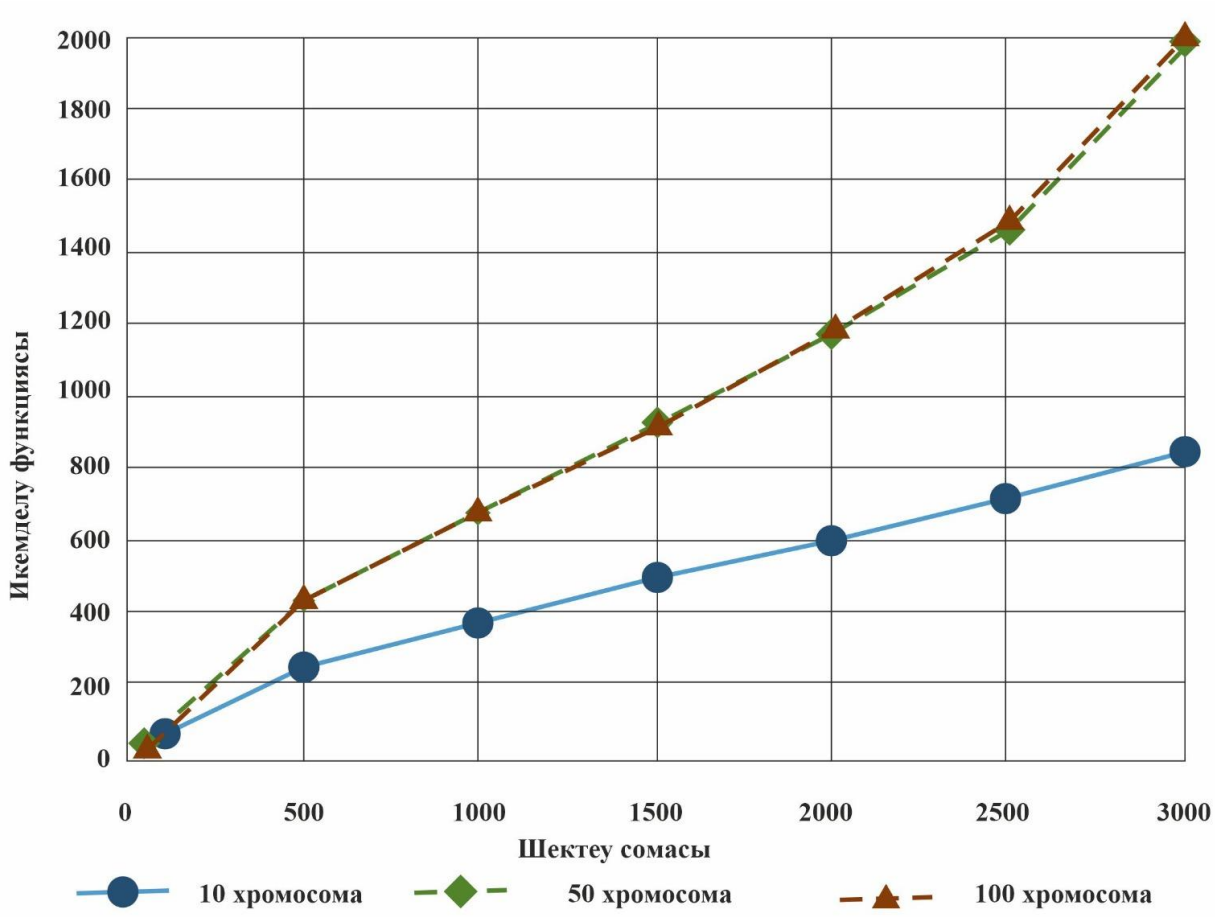
Рюкзакқа арналған жиынтық, яғни талданатын АКЖ түйіні 3.6-суреттегі форманың оң жағындағы кестеде көрсетілген. Яғни, іс жүзінде мультирюкзак қалыптастыру есебі шешіледі. ШҚҚЖ объектіге бағытталған тәсілді пайдалана отырып әзірленген.

Модификацияланған ГА+ШБӘ есептеу ядро мұнда қолданылған стандартты ГА-дан мынадай белгілермен ерекшеленеді: хромосомалар матрицалар түрінде ұсынылған, олардың элементтері АКЖ түйіндеріндегі АҚҚ нөмірлеріне сәйкес келетін сандар болып табылады; *k*-нүктелі кроссинговер қолданылды.

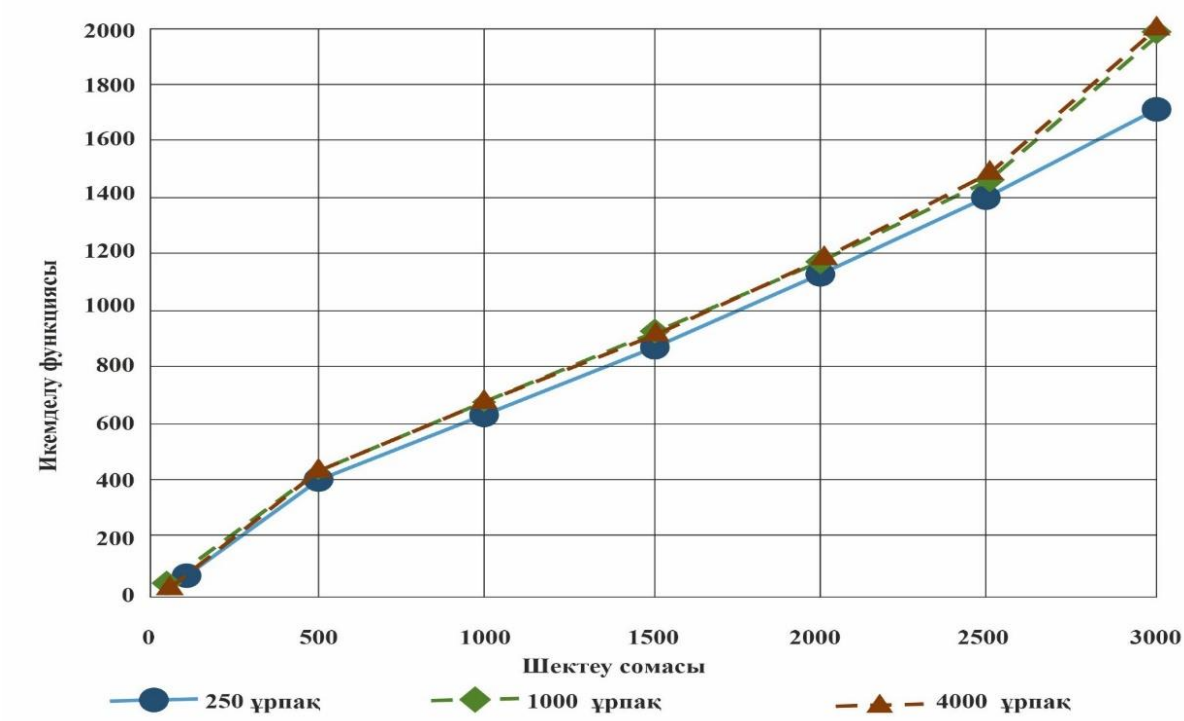
Ауыспалы мутация қолданылды, яғни мутация ықтималдығы қажеттілікке байланысты ГА жұмыс барысында икемделу түрінде өзгеруі мүмкін. Икемделу функциясы ұтымдылық коэффициенттерінің қосындысы ретінде ұсынылған. Бұл ретте, АҚҚ тиімділігінің дәстүрлі абсолютті көрсеткіштерінен (интегралдық көрсеткіште интеграцияланған) басқа, ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасы, сондай-ақ АҚҚ-ның әрбір класы үшін құндық көрсеткіштері ескеріледі.

АКЖ түйіндері бойынша АҚҚ орналастыруды көп критерийтық ұтымды шешу бойынша алгоритм мен ШҚҚЖ барабарлығын тексеру үшін тиісті есептеу эксперименттері жүргізілді, 3.7–3.10-суреттерді қараңыз.

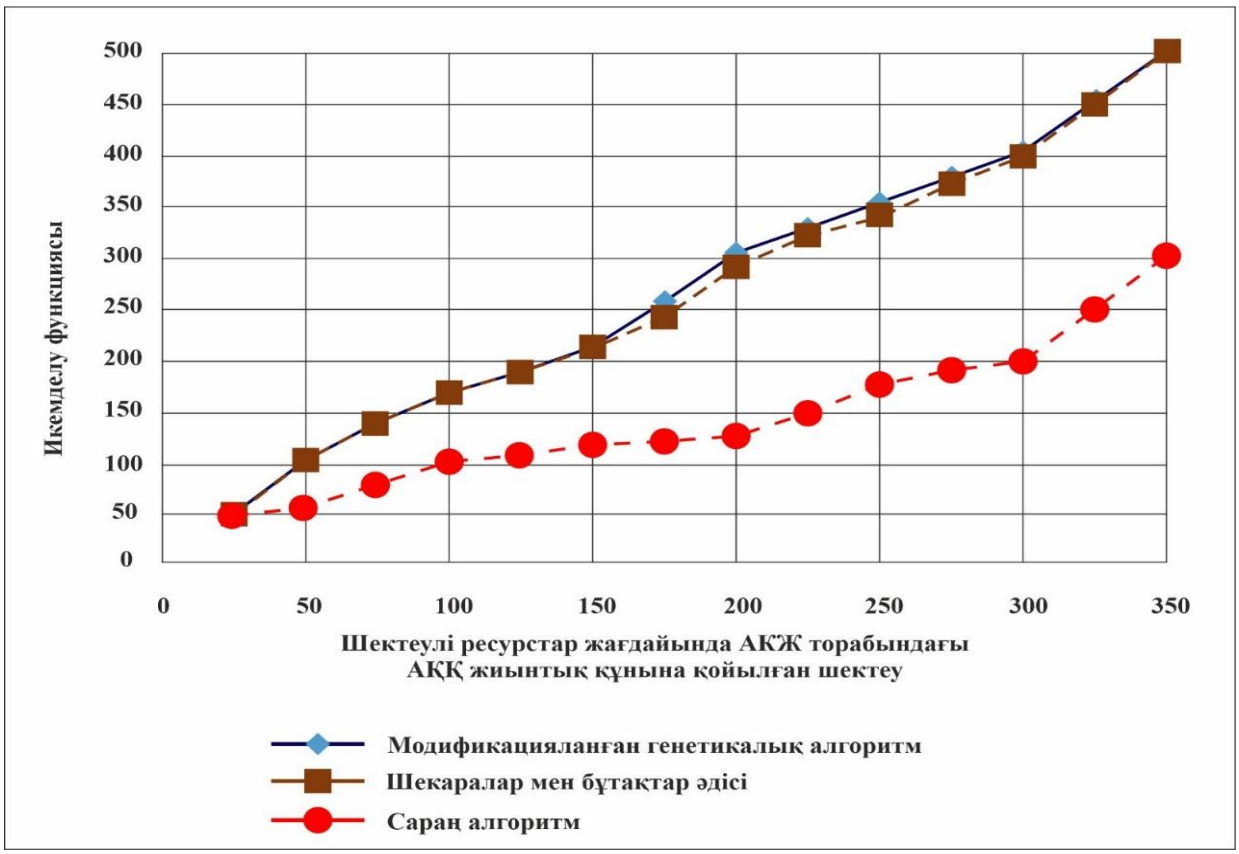
Есептеу эксперименттері кездейсоқ құрылған АҚҚ жиынтығы үшін жүргізілді. Модификацияланған (құрама ГА+ШБӘ), бұтақтар мен шекаралар әдісі және сараң алгоритмі жұмыстарының тиімділігі салыстырылды.



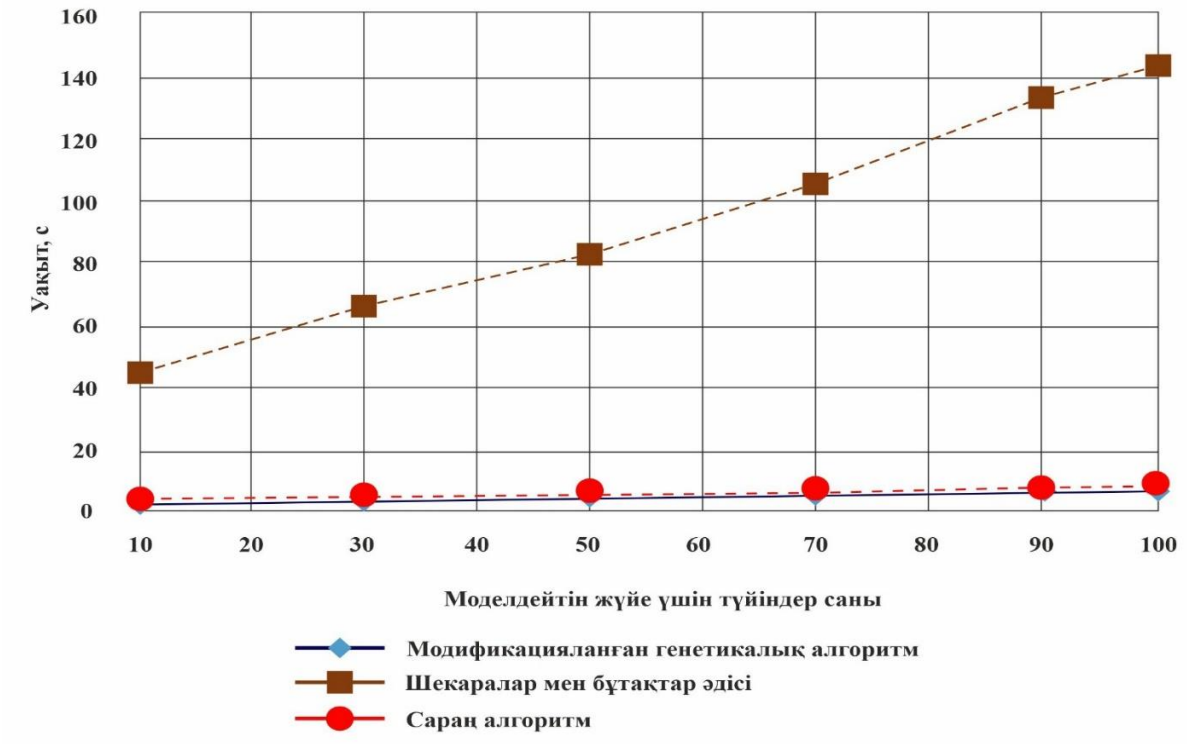
3.7-сурет – Популяциядағы хромосомалардың әртүрлі саны үшін алгоритмнің тиімділігін салыстыру



3.8-сурет – Әртүрлі ұрпақтар үшін алгоритмнің тиімділігін салыстыру



3.9-сурет – ШҚҚЖ пайдаланылатын алгоритмдердің тиімділігін салыстыру бойынша есептеу эксперименттерінің нәтижелері



3.10-сурет – Алгоритмдер жұмыс уақытын салыстырғанда есептеу эксперименттер нәтижелері

3.7-суреттің графигінде популяциядағы хромосомалардың ұтымды санын іздеу барысында АКЖ-ға арналған ақпаратты қорғаудың ұтымды жиынтығын іздеу есебін шешу үшін ГА зерттеу нәтижелері көрсетілген. Есептеу эксперименттері көрсеткендей, егер хромосомалардың саны үлкен болмаса (20-дан аз) ұтымды нәтижеге қол жеткізу мүмкін емес. Алайда, олардың саны 22-25-тен асқан кезде алгоритмнің тиімділігі жоғарылаған жоқ. 500-ден астам есептеу эксперименттерінің сериясы негізінде алгоритмнің соңғы нұсқасы және оны бағдарламалық іске асыру үшін популяцияда 25 хромосоманы алу жеткілікті екендігі анықталды [87].

Қарастырылып отырған ГА+ШБӘ үшін ұрпақтардың ұтымды санын іздеу барысында бірқатар есептеу эксперименттері жүргізілді, 3.8-суретті қараңыз. Тексеру барысында ГА+ШБӘ тиімділігі 450-500 ұрпақ шебінен өткеннен кейін артпайтыны анықталды. Бұл жағдай біздің ШҚҚЖ үшін 500 ұрпақ санымен ГА+ШБӘ-дағы ұрпақтар санын шектеуге негіз береді.

Есептеу эксперименттері барысында ГА + ШБӘ өте жоғары ұтымдылықпен, сондай-ақ жылдамдығымен ерекшеленетіні анықталды, 3.9, 3.10-сур. қараңыз.

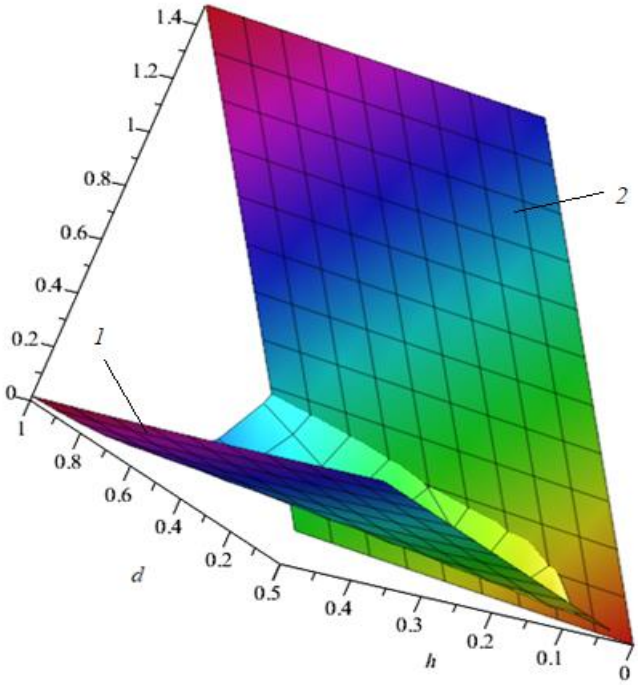
ГА+ШБӘ пайдалану кезінде есепті шешуге жұмсалған уақыт бұтақтар мен шекаралар әдісінің көрсеткіштерімен салыстырғанда шамамен 16-25 есе аз екендігі анықталды. Сараң алгоритм үстеме шектеулер мен айнымалылар санын ескере отырып, көп критерийлі ұтымды шешу есебін икемделу тұрғысынан ГА-дан да, бұтақтар мен шекаралар әдісінен де айтарлықтай төмен.

Осылайша, талдау әзірленген модельдер мен алгоритмнің сенімді екендігін және есептеу эксперименттерінің нәтижелері бірнеше рет практикалық іске асырулармен расталғанын көрсетеді [87, 2-б].

ГА және оның модификациясын тиімді пайдалану үшін ГА+ШБӘ комбинациясын қолдану арқылы алдымен АҚҚ жиынтығына ақпаратты қорғауға арналған ең өнімді құралдар мен металарды таңдау қажет екендігі көрсетілген. Жоғарыда қарастырылған интегралды көрсеткіш талданған АКЖ түйіндері үшін қорғаныс құралдары мен шараларын таңдауда маңызды рөл атқарады. Бұл көрсеткіш (ИнК) диссертациялық зерттеу контексінде нақты АҚҚ-ның аса маңызды сипаттамалары сапасының жалпыланған көрсеткіші ретінде түсіндіріледі. ИнК АОБ үшін АҚҚ шығындарының өнімділік параметрлерімен тікелей байланысты болғандықтан (диссертацияның екінші тарауында қарастырылған), АКЖ түйінінде АҚҚ-ның тиімді жиынтығын қалыптастыру, Егер белгілі бір АҚҚ үшін қажетті мақсаттарға қол жеткізу дәрежесі жоғары болса, қорғау тарапының ресурстарды бөлу бойынша артық шығындардан аулақ болады.

Енді АКЖ түйіні үшін АҚҚ іріктеудің ұтымды шешу есебін шешу үшін модификацияланған ГА қолданудың тиімділігі расталған кезде қауіптерді іске асырудан келтірілген залалды сипаттайтын мақсат функцияларды – өрнек (2.7), сондай-ақ қорғау түйіні АҚҚ инвестициялау стратегияларын таңдауды сипаттайтын функцияларды ұтымды шешу үшін ГА қалай жұмыс істейтінін көруге болады.

3.11-суретте екі беттің қиылысында құрылған мақсатты функцияны қалыптастыру мысалы көрсетілген: 1 – объектінің осалдығын сипаттайтын функция үшін және 2 – қорғау жағынан АҚҚ-ға инвестициялаудың ұтымды стратегиясын сипаттайтын функциялар [87, 3-б].



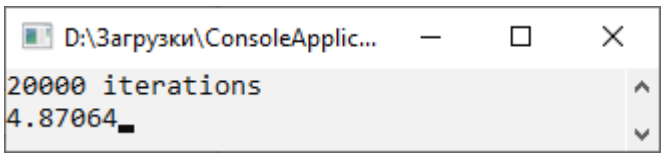
3.11-сур – Екі беттің қиылысында құрылған мақсатты функцияны қалыптастыру: (1) – объектінің осалдығын сипаттайтын функция үшін және (2) - қорғау тарапынан АҚҚ-ға инвестициялаудың ұтымды стратегиясын сипаттайтын функция.

Осы функциялардың әрқайсысы үшін экстремумдарды іздеуді ГА-ны қолдануға жүгіну арқылы ұйымдастыруға болады.

Мысалы, егер қорғаныс жағы үшін АҚҚ-да инвестициялардың мөлшерін $const = 1$ (қорғаныс құралдары - $const = d$) тең қабылдайтын болсақ, онда икемделу функциясын (с++) модельдеу үшін ГА-ны келесі консольдік іске асыруды аламыз.

$v(h,d) = r^n \big/ \left(r^n + a\right)$, үшін $r = \left(h \big/ d\right)$, $n = 3, a = 8$. Инвестиция кілт жоғалған (немесе бұзылған) сәтке дейін нәтиже бермейтін жағдай. Осыдан кейін криптожүйенің осалдығы күрт артады. *n* шамасы неғұрлым үлкен болса, кедергі шабуылдарға аз әсер ететін шекті мән соғұрлым үлкен болады. Сонымен қатар, қорғаныс жағы мен шабуылдаушылар ресурстарының арақатынасы шекті мәннен асқан кезде өсу аймағы соғұрлым тез артады.

ГА жүзеге асыру нәтижесінде келесідей нәтижеге қол жеткіземіз, 3.12-суретті қараңыз.



3.12-сурет – Бір айнымалы функцияны ұтымды шешу нәтижесі (қорғаныстың тұрақты ресурстары кезінде шабуылдаушы тараптың ресурстары)

Алынған нәтиже шабуыл объектісі мен оның ақпараттық ресурстары осал болуы мүмкін екенін білдіреді, егер шабуылдаушы тарап осы АҚҚ-ны жеңуге өз салымдарын шамамен бес есе арттыруды қамтамасыз ете алатын болса. Мысалда АОБ үшін АҚҚ шығындарының өнімділік параметрлері қабылданады. Бұл мәндер сынақ болып табылады және зерттеу нәтижелері бойынша қабылданады. Бұл сынақ мысалында олар ақпаратты қорғаудың шартты құралдарының ұтымдылық көрсеткіштері мен оларды сатып алу, қызмет көрсету, модернизациялау шығындарының коэффициенттерін сипаттайды.

Диссертациялық зерттеудің 4-ші қорытынды тарауы АОБ үшін АҚ және КҚ көп контурлы жүйелерінің ұтымды конфигурацияларын іздеу, сондай-ақ қолданыстағы қауіптердің өзектілігіне сүйене отырып, қорғау тарапының ресурстарын ұтымды қайта бөлу жөніндегі есепті шешу үшін модификацияланған ГА (ГА+ШБӘ) қолдану бойынша ШҚҚЖ әзірлеудің практикалық аспектілеріне арналған [88].

3.3. 3-тарау бойынша қорытындылар

1. Ақпараттық-коммуникациялық жүйелердің қауіпсіздік контурлары үшін ақпаратты қорғау құралдарының (АҚҚ) конфигурацияларының нұсқаларын іріктеумен және ұтымды шешумен байланысты есепті шешу үшін генетикалық алгоритмді (ГА) түрлендіру мүмкіндігі қаралды. Жұмыстың осы бөлімінде алынған нәтижелердің ғылыми жаңалығы ГА-да АҚҚ құрамын ұтымды шешу үшін өлшемдер ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасын, АҚҚ интегралды көрсеткіштерін, сондай-ақ әрбір АҚҚ сыныбы үшін құндық көрсеткіштерді пайдалану ұсынылатындығында. АКЖ-қа арналған АҚҚ құрамын таңдауды ұтымды шешу есебіндегі генетикалық алгоритм көп таңдаумен байланысты есептің вариациясы ретінде қарастырылады. Бұл өндірісте АҚҚ-ны АКЖ-қорғаныс контурлары бойынша орналастыруды ұтымды шешу рюкзактың комбинаторлық есебін өзгерту ретінде зерттеледі. Ұсынылған тәсіл АКЖ түйіндерінің әрқайсысы үшін АҚҚ жиынтығын ұтымды шешу жөніндегі көп критерийліесепті шешуге ғана емес, сонымен қатар АОБ КҚ-ға бөлінетін ресурстардың шектеулілігі жағдайында қорғау тарапының ресурстарын қайта бөлудің орындылығына жедел талдау жүргізуге мүмкіндік береді.

2. Зерттеудің практикалық құндылығы ақпараттың жоғалуынан болатын қауіптердің жалпы мөлшерін, АҚҚ интегралды көрсеткіштерін, сондай-ақ АҚҚ-

ның әрбір класы үшін құндық көрсеткіштерді ескере отырып, ГА-ның ұсынылған модификациясы негізінде шешім қабылдауды қолдау жүйесіне есептеу өзегі үшін ұтымды қосылатын кітапхана түрінде модульді бағдарламалық іске асыру болып табылады.

3. ГА және бұтақтар мен шекаралар әдісінің артықшылықтарын біріктіретін модификацияланған құрама алгоритмді іске асырудың ұтымды бағдарламалық алгоритмін таңдау бойынша есептеу эксперименттері жүргізілді.

4. Әзірленіп жатқан ШҚҚЖ үшін ұтымды нұсқа ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамаларын, АҚҚ интегралды көрсеткіштерін, АҚҚ-ның әрбір класы үшін құндық көрсеткіштерін ескеретін, сондай-ақ ГА мен ШБӘ-ның барлық оң жақтарын біріктіретін ГА модификациясын пайдалану керек екендігі көрсетілген.

5. Модификацияланған ГА-ны іске асыру АКЖ-қа арналған КҚ құралдарын орналастырудың ұтымды нұсқаларын іздестіруді жеделдетуге, сондай-ақ қорғау ресурстарын олардың шектеулілігі жағдайында қайта бөлу жөніндегі есепті шешуге мүмкіндік беретіні көрсетілді. Бұл артықшылық аппараттық және бағдарламалық жасақтаманың әртүрлі нұсқаларын және олардың АКЖ-ге арналған комбинацияларын жылдам сұрыптауға ғана емес, бірақ кейінірек тарауда келтірілген модельдер мен алгоритмдерді қолданыстағы модельдермен және АКЖ киберқауіпсіздік контурларының құрамын ұтымды шешу алгоритмдерімен біріктіруге де жағдай жасайды. Модельдер мен алгоритмдердің мұндай бірігуі АКЖ қорғанысын тез қалпына келтіруге мүмкіндік беретіндігі ықтимал.

4 ҚОРҒАУ ОБЪЕКТІЛЕРІ АРАСЫНДА РЕСУРСТАРДЫ БӨЛУДІ ҰТЫМДЫ ШЕШУ БАРЫСЫНДА ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУДЫҢ МОДУЛЬДІК ЖҮЙЕСІН ӘЗІРЛЕУ

Шешім қабылдау процесінің үнемі күрделенуі, атап айтқанда басқарушылық, әртүрлі АОБ үшін КҚ қамтамасыз ету есептерін, сондай-ақ шешімдерге әсер ететін факторлардың өзара байланысын қамтитын пәндік салалардың күрделілігімен бірге шешім қабылдауды қолдау үшін сыртқы құралдарды тарту қажеттілігін анықтайды. Нашар құрылымдалған пәндік салаларда (мысалы, АТ-ға инвестициялау, киберқауіпсіздік, атап айтқанда, ақпаратты қорғау тарабының ресурстарын ұтымды қайта бөлу және т.б.), детерминистік ақпаратты шешім қабылдау үшін жеткілікті мөлшерде алу мүмкіндігі болмаған жағдайда, шешім қабылдауды сараптамалық қолдау олардың сапасын арттырудың жалғыз құралы болып табылады. Бұл, негізінен, жоғары ұйымдастырушылық деңгейлердің есептерін шешу туралы (мысалы, маңызды АОБ ақпараттық жүйелері), дұрыс емес шешімнің «бағасы» қазіргі уақытта тым жоғары және үнемі өсіп келеді. Егер әртүрлі АОБ үшін киберқауіпсіздік ресурстарын ұтымды басқару есептеріндегі шешімдерді қолдау туралы айтатын болсақ, онда хакерлер тарапынан мемлекеттік және жеке компаниялардың ат инфрақұрылымына деструктивті әсердің саны мен күрделілігінің қарқынды өсуімен бірге ресурстарды бөлу стратегиясын дұрыс

таңдау ақпараттық массивтердің, беделдің жоғалуына ғана емес, сонымен қатар кибершабуыл объектісін қаржыландыруға айтарлықтай зиян келтіруі мүмкін.

4.1. Ақпараттандыру объектілерінде ақпаратты қорғау тарапының ресурстарын бөлу есебі үшін ОҚҚЖ тұжырымдамалық жобалау

Нақты ақпараттандыру объектісі үшін ақпаратты қорғау тарабының ресурстарын бөлу процесінде шешімдер қабылдауды қолдау жүйесі (бұдан әрі – ШҚҚЖ) оны кез келген мүдделі тұлғалардың барлық мекемелерде немесе кәсіпорындарда пайдалануы мақсатында құрылады, олар үшін қорғаныс жағының ресурстарды бөлудің ұтымды стратегиясын табу есебі компьютерлік зиянкестердің ақпараттық ресурстарға деструктивті әсер етуінің саны мен күрделілігінің артуы жағдайында өзекті болып табылады.

ШҚҚЖ келесі есептерді шешуге бағытталған:

- білім (ББ), мәліметтер (МБ) базаларын, ақпаратты қорғау тарабының ресурстарын бөлу стратегиясын таңдаумен байланысты әртүрлі жағдайлар бойынша база құру, пайдаланушылардың қолжетімділігін шектей отырып, АОБ қорғау тарабының ресурстарын ұтымды бөлу стратегияларының бірыңғай электрондық мұрағатын жүргізу үшін бағдарламалық қамтамасыз етуді әзірлеу;
- ақпаратты қорғау тарабының ресурстарын бөлудің ұтымды стратегияларын есепке алу, деректер форматтары мен алмасу хаттамаларын ішкі стандарттау есебінен ШҚҚЖ кіші жүйелері арасындағы ақпараттық өзара іс-қимылды қамтамасыз ету саласында бірыңғай ақпараттық кеңістік құру;
- ақпаратты қорғау тарапының ресурстарын бөлудің ұтымды стратегияларын таңдау бойынша шығыс құжаттамасын қалыптастырудың бірыңғай жүйесін құру;
- шешім қабылдайтын тұлғаға (ШҚТ) қажетті құжаттардың үлгілері мен шаблондарының ДБ жүргізу;
- шешім қабылдау үшін аналитикалық ақпаратты графикалық және баспа түрінде қалыптастыру;
- ақпараттандыруды дамытудың жүйелілігін, кешенділігін және келісімділігін қамтамасыз ету, сүйемелдеу мен бақылаудың дәстүрлі объектілері мен әдістерін пайдалана отырып, ақпаратты қорғау тарапының ресурстарын бөлу есептері.

Ақпараттық және кибернетикалық қауіпсіздік бағдарламалары үшін ШҚҚЖ-ның негізгі функциялары, әдетте, мыналарды сақтау қажеттілігіне қарай регламенттеледі: КҚ проблематикасын кешенді талдау принциптері; шешімдерді қолдау процесінде қолданылатын ресми және бейресми әдістерді біріктіру мүмкіндіктері; есептің ағымдағы жағдайына қатысты ақпараттың сенімділігі мен өзектілігі принциптері. Бұл ретте, әдетте, әртүрлі есептерді, статистикалық деректерді, талдамалық шолуларды, сондай-ақ мониторингтің кіші жүйелерінен алынатын деректерді пайдаланады; шешім қабылдауды интеллектуализациялау үшін әдістер мен модельдерді автоматтандырылған таңдау принциптері; ШҚҚЖ жағдайын одан әрі дамыту қағидаттары; ШҚҚЖ жұмыс істеу тиімділігін және қабылданған ұсыныстар мен қорытындылардың негізділігін арттыру мақсатында

ШҚҚЖ-ны ұтымды басқару қағидаттары, оларды шешім қабылдаушы тұлғаның бақылау іс-шараларын әзірлеу процесінде пайдалана алады; талдау, жедел басқару және шешілетін тапсырманы бақылау модульдерінің әлеуеті.

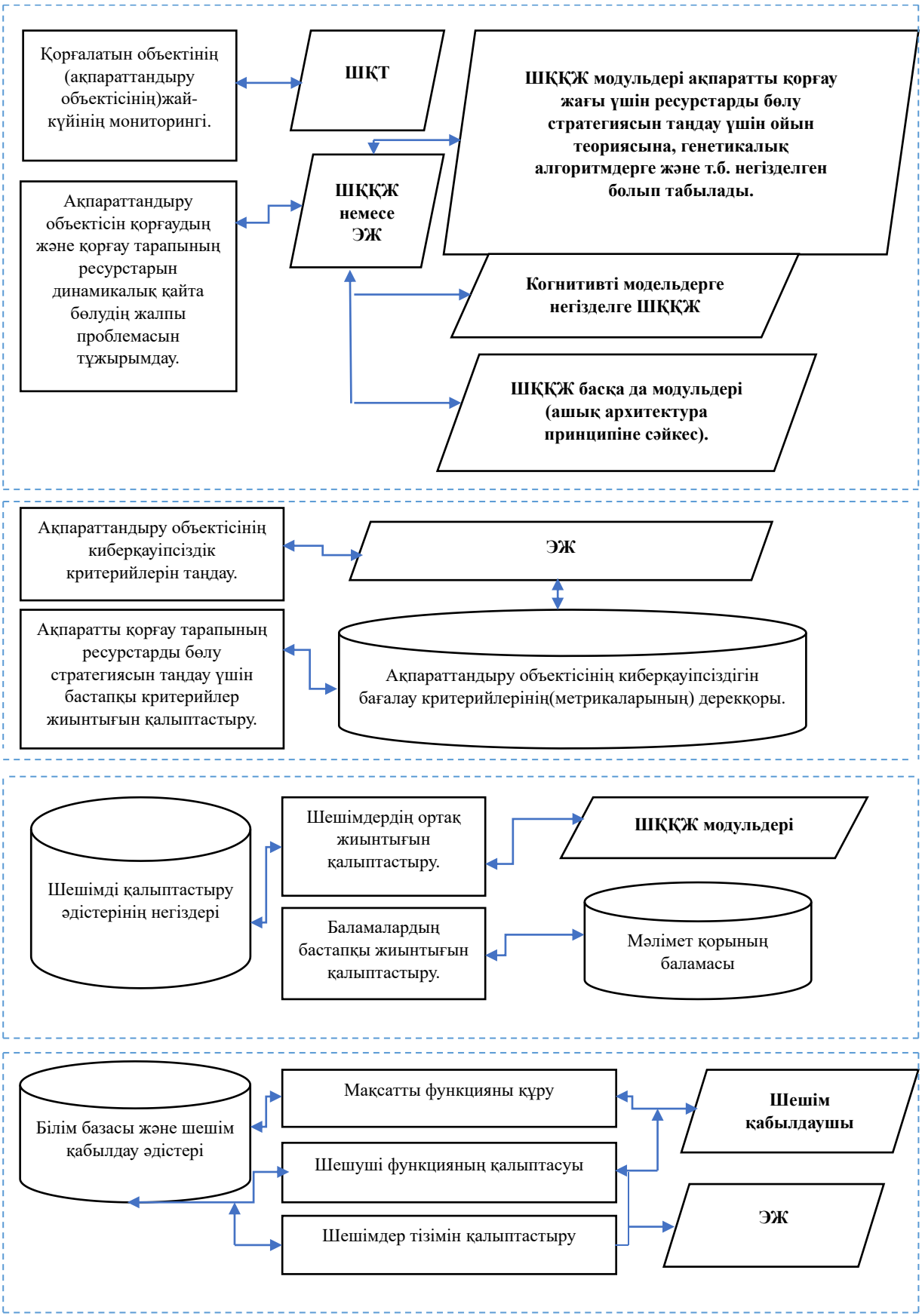
ШҚҚЖ толық жұмыс істеуін қамтамасыз ету үшін, әдетте, мынадай негізгі модульдер мен кіші жүйелерді қамтуы тиіс, 4.1-суретті қараңыз:

1. Шешім қабылдау үшін қолданылатын МБ, ББ, модельдер мен ережелер базасы.

2. Интерфейсті басқару жүйесі. Ол ШҚҚЖ архитектурасы – жергілікті немесе клиент-серверлік негізінде жобаланады.

3. Басқа модульдер мен ішкі жүйелер, олардың қажеттілігі пәндік аймақтың ерекшелігімен байланысты.

ШҚҚЖ шешім қабылдауды қолдаудың келесі түрлерін қамтамасыз етуі керек: сараптамалық қолдау; автоматтандырылған шешім шығару; аралас шешім.



4.1-сурет – Ақпаратты қорғау тарабының ресурстарын бөлудің ұтымды стратегиясын таңдауға қатысты шешімдер қабылдау процесіндегі ШҚҚЖ архитектурасы.

ШҚҚЖ (немесе ЭЖ) өзегі білім базасы (ББ) болып табылады. Осы пәндік ББ-да ақпаратты қорғау тарабының ресурстарын ұтымды бөлу есептеріндегі сарапшылардың білімі жинақталатын болады. Білімді эвристикалық ережелер форматында ұсынған жөн.

ББ-да оқыту және жаңа білім жинақтау келесідей:

ақпаратты қорғау тарабының ресурстарын ұтымды бөлудің нақты есебін қарау кезінде оны шешуді қамтамасыз ететін ереже қалыптастырылады;

әзірленген ережелер нақты тапсырманың ерекшелігіне байланысты ережелер базасына орналастырылады.

ШҚҚЖ ереже базасында қажетті ережені іздеу, мысалы, семантикалық модельдер негізінде жүзеге асырылады.

«Ақпараттандыру объектісінің ақпараттық ресурстарын ұтымды бөлу проблемалары мен тәуекелдерін талдау» ішкі жүйесінің жұмыс істеу алгоритмінің блок-схемасы 4.2-суретте көрсетілген.

Ақпаратты қорғау тараптарының ресурстарын ұтымды бөлу кезінде жиі кездесетін есептердің төрт класы бар:

1. Стандартты есептер. Бұл кластың есептері, әдетте, ШҚТ белгілеген нұсқауларды қолдануды қажет етеді.

2. Жақсы құрылымдалған есептер. Бұл кластың есептері сандық сипаттамалар мен көрсеткіштерге ие. Есептердің осы класын шешу үшін, әдетте, экономикалық және математикалық әдістер қолданылады.

3. Нашар құрылымдалған есептер. Бұл кластың есептері сандық ғана емес, сонымен қатар сапалық сипаттамаларға ие. Мұндай есептерді шешу үшін жүйелі талдау әдістерін ШҚҚЖ-ға қолдану қажет.

4. Құрылымданбаған есептер. Мұндай есептерді шешу белгілі бір пән саласына сарапшылар тарту қажеттілігін тудырады.

«Ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын ұтымды бөлу үшін проблемалар мен тәуекелдерді талдау» кіші жүйесі есептелі одан әрі шешу мақсатында оны іздестіруді және тұжырымдауды қамтамасыз етуге тиіс. Осы ішкі жүйені іске қосудың негізгі бағыттары:

ақпаратты қорғау тарабының ресурстарын ұтымды бөлу объектілерінің мониторингі;

АОБ ақпаратын қорғау тарапының ресурстарын ұтымды бөлу үшін сандық критерийтар мен көрсеткіштерді айқындау;

аргументтер негізінде АОБ ақпаратын қорғау тарабының ресурстарын ұтымды бөлуді іске асырумен есептер көздерін айқындау;

ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын ұтымды бөлуге байланысты есепті тұжырымдау әдісін таңдау;

жалпы есепті тұжырымдау;

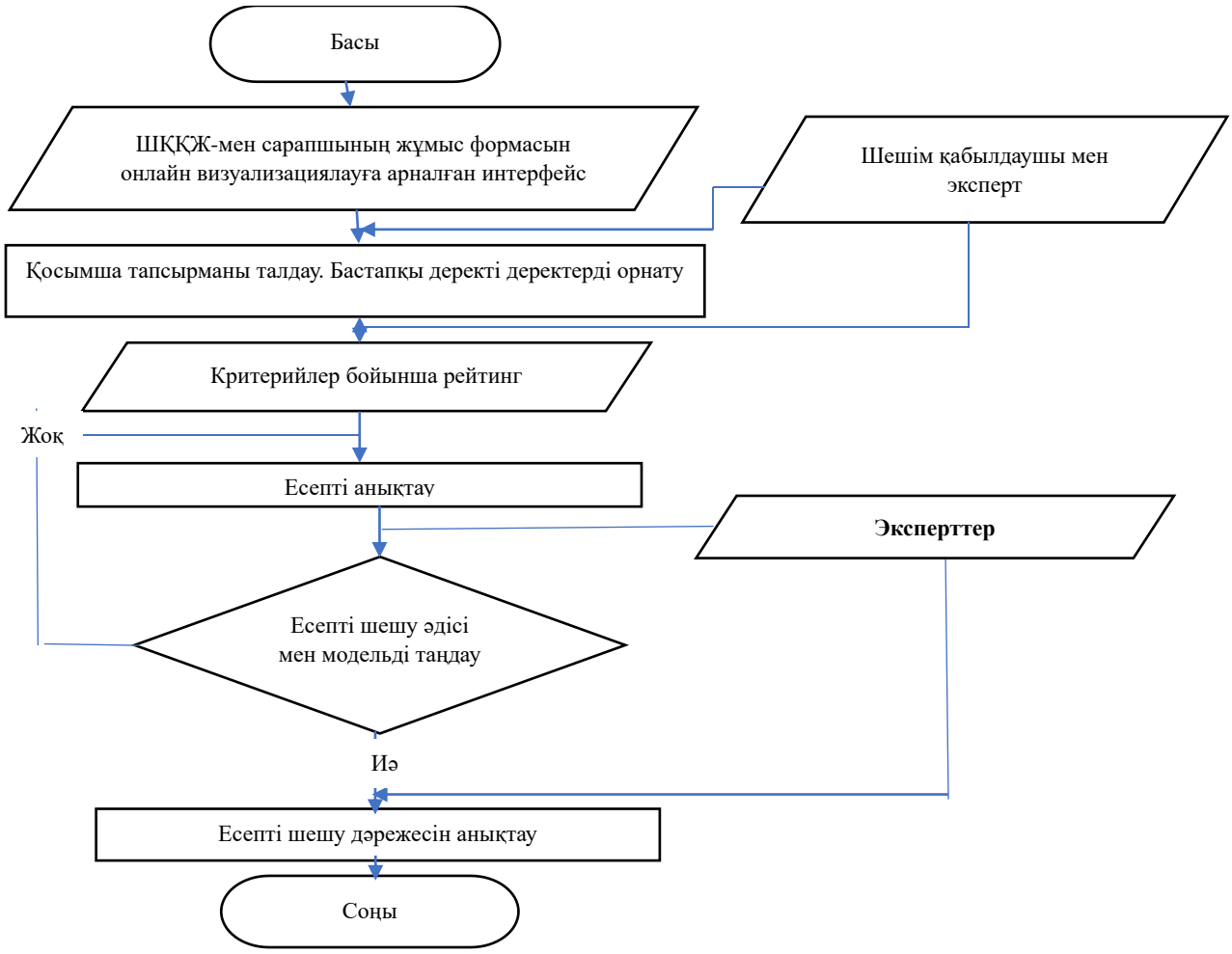
есептің белгісіздік дәрежесін анықтау;

жалпы есеп шеңберіндегі жеке есептерді анықтау.

Есепті анықтағаннан кейін ақпараттандыру объектісінің ақпаратын қорғау тарапының ресурстарын ұтымды бөлуді іске асыру тиімділігінің мақсаттар тізбесін және критерийтар жүйесін қалыптастыру қажет. Бұл есепті кейіннен бағалау және оны одан әрі шешу жолдарын табу үшін қажет. Ол үшін ШҚҚЖ-

да «АОБ ақпаратын қорғау тарабының ресурстарын ұтымды бөлу стратегиясын бағалау үшін мақсаттар мен өлшемдер жүйесін қалыптастыру» деген жеке кіші жүйе бар, 4.3-суретті қараңыз.

АОБ ақпаратын қорғау тараптарының ресурстарын ұтымды бөлу кезінде қол жеткізуге болатын мақсатты немесе көптеген мақсаттарды қалыптастыру кезінде әртүрлі есептер туындауы мүмкін. Бұл есептер біріктірілуі; бір-біріне қайшы келуі; өзара ерекше болуы және т. б. мүмкін.



4.2-сурет – «Ақпараттандыру объектісі ақпаратын қорғау тарабының ресурстарын ұтымды бөлу есебі үшін проблемалар мен тәуекелдерді талдау» кіші жүйесінің жұмыс істеу алгоритмінің блок-схемасы

АОБ ақпаратын қорғау тараптарының ресурстарын ұтымды бөлудің ұтымды стратегиясын іздеу, ұтымдылықты бағалау критерийлерінің мақсаттары мен жүйесін қалыптастыру сияқты күрделі проблематиканы: сарапшылар тұжырымдайтын қағидатты жаңа новаторлық мақсаттарға; ұқсас жағдайларда туындаған мақсаттарға ұқсас типтік мақсаттарға; нақты ШҚҚЖ үшін генерациясы қолжетімді құрамдастырылған мақсаттарға бөлген жөн.

Мақсаттар мен ұтымдылық критерийлерін қалыптастырудың ең тиімді әдісі сарапшылармен өзара әрекеттесетін бағдарламалық жүйелер болып табылады.

«АОБ ақпараттарын қорғау тарабының ресурстарын ұтымды бөлу стратегиясын бағалау үшін мақсаттар мен өлшемдер жүйесін қалыптастыру» кіші жүйесі ШҚҚЖ-ның одан әрі жұмыс істеуі үшін мақсаттар мен критерийтар жүйесін кезең-кезеңімен қалыптастыруды қамтамасыз етуі тиіс. Сонымен қатар, бұл ішкі жүйеде мыналар іске асырылды:

ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын ұтымды бөлу тиімділігінің критерийлері мен көрсеткіштерінің көп деңгейлі иерархиясы;

қосалқы мақсаттар үшін критерийтарды декомпозициялау мүмкіндігі;

ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын ұтымды бөлу тиімділігінің критерийлері мен көрсеткіштері арасындағы математикалық тәуелділіктерді анықтау мүмкіндіктері;

ақпараттандыру объектісінің ақпаратты қорғау жағынан ресурстарды ұтымды бөлу үшін ШҚҚЖ ұсынған стратегияны көрнекі бағалау үшін шкалаларды, өлшем бірліктерін және маркерлерді таңдау мүмкіндігі.

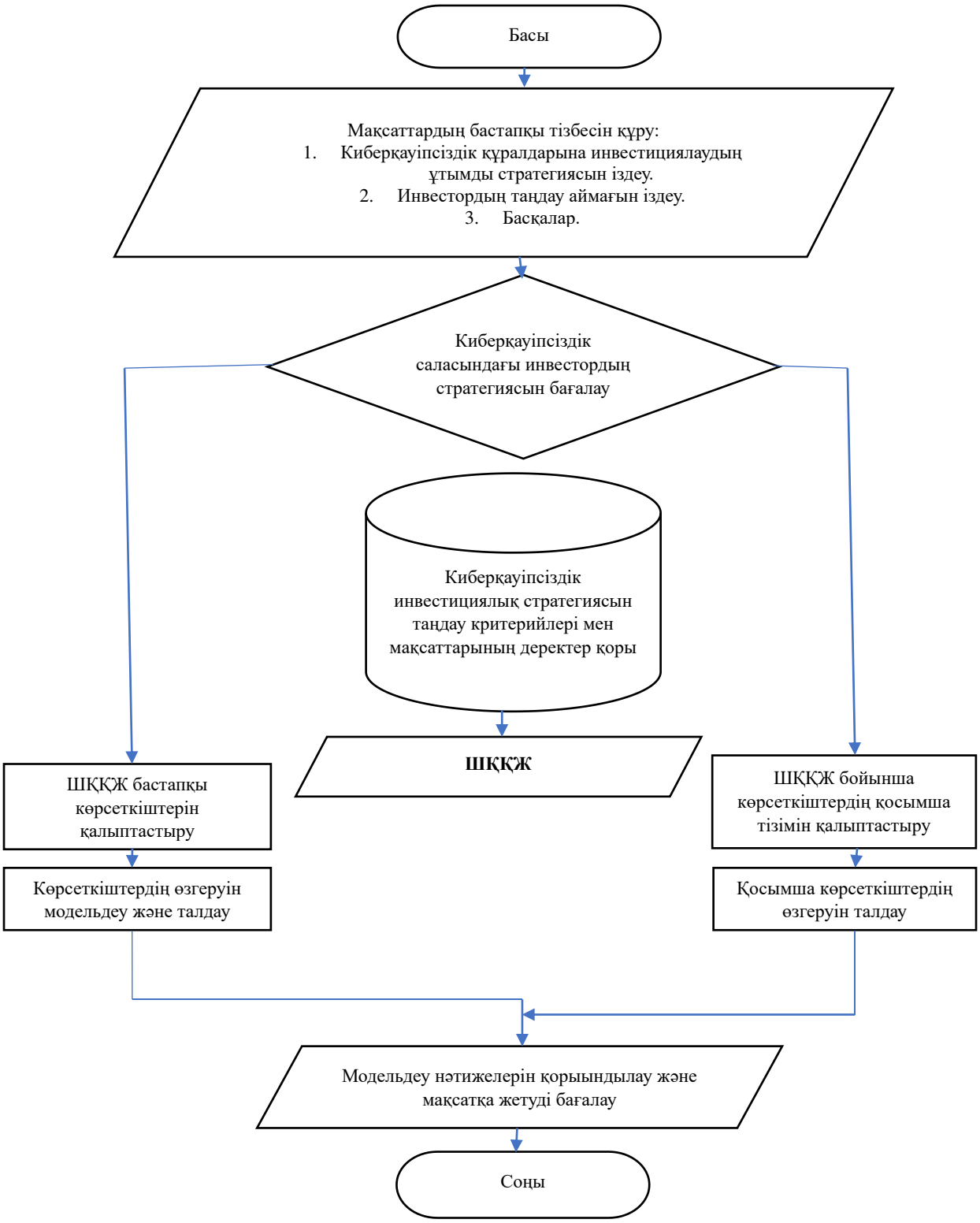
Ақпараттандыру объектісінің ақпаратын қорғау тарапының ресурстарын ұтымды бөлудің ұтымды стратегиясын таңдау есебін одан әрі талдау үшін шешімдердің баламалы нұсқаларын қалыптастыру қажет.

Бұл баламалы нұсқалар «Ақпараттандыру объектісінің ақпаратты қорғау тарабының ресурстарын ұтымды бөлу процесінде қабылданатын шешімдерді қалыптастыру» кіші жүйесінде қалыптастырылатын болады.

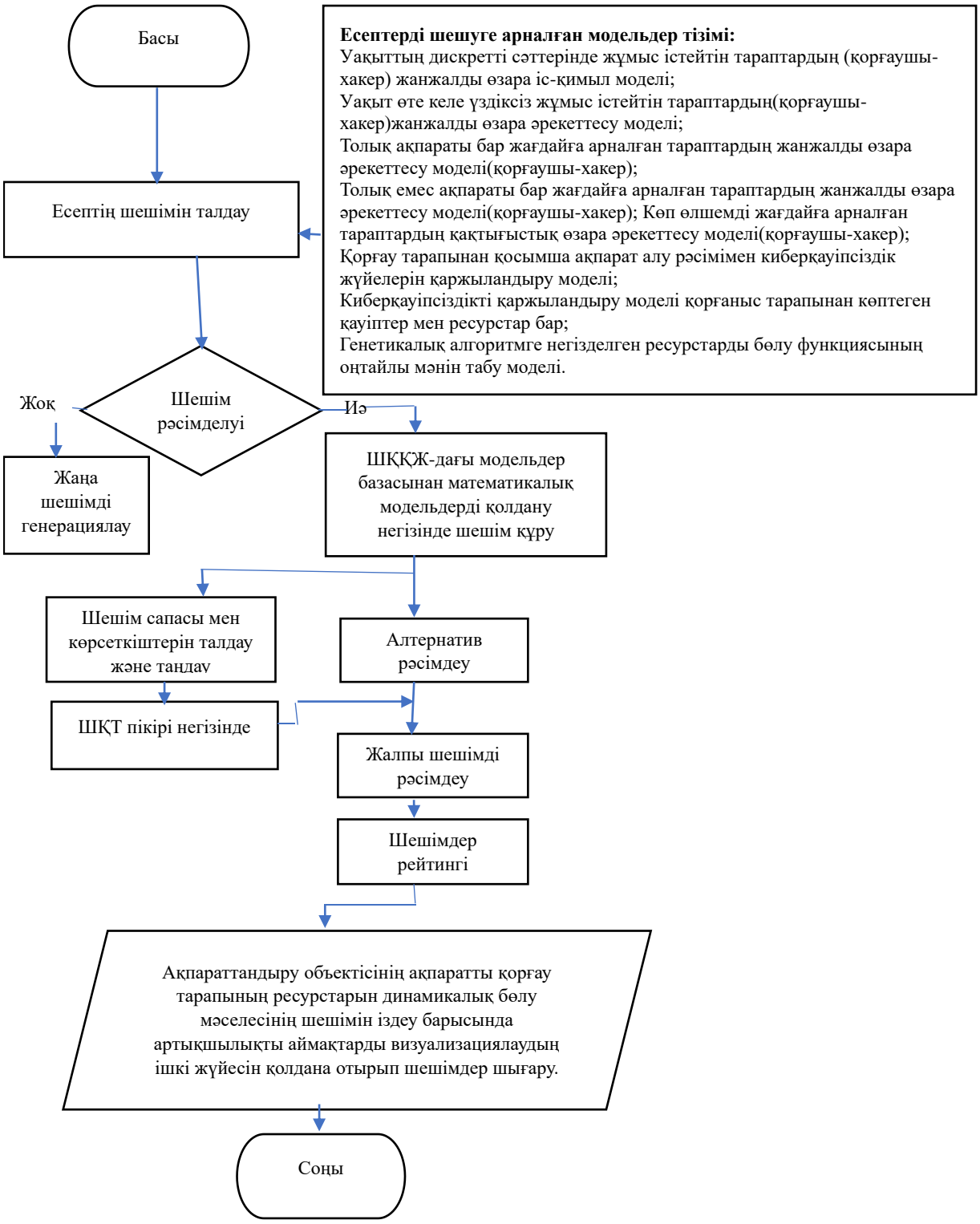
«Шешімдерді қалыптастыру» ішкі жүйесінің жұмыс істеу алгоритмінің блок-схемасы 4.4-суретте көрсетілген.

АОБ қорғаныс жағының ресурстарын ұтымды бөлудің ұтымды стратегияларын іздеу есептеріне арналған мүмкін шешімдерді қалыптастыру қазіргі уақытта ойын теориясының немесе ұтымды бағдарламалаудың математикалық аппаратын қолдану негізінде жүзеге асырылады.

АОБ қорғау жағының ресурстарды ұтымды бөлудің ұтымды стратегиясын таңдау: жоғарыда 2 және 3-тарауларда ұсынылған аналитикалық модельдерді бағдарламалық қамтамасыздандыру арқылы жүзеге асырылады. Бұл жүйелердің сараптамалық кіші жүйелерін пайдалану арқылы; шешім қабылдаушы тұлға (ШҚТ) берген немесе ШҚҚЖ білім базасынан алынған түрлі модельдердің комбинациясы арқылы сценарийлер құру арқылы орындалды.



4.3-сурет – Кіші жүйенің жұмыс істеу алгоритмінің блок-схемасы «Ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын ұтымды бөлу стратегиясын бағалау үшін мақсаттар мен критерийтар жүйесін қалыптастыру»



4.4-сурет . АОБ қорғау тарабының ресурстарын ұтымды бөлу процесінде қабылданатын шешімдерді қалыптастыру кіші жүйесінің жұмыс істеу алгоритмінің блок-схемасы

Шешімдерді қалыптастыру процесі екі түрге бөлінеді: әзірге ШҚҚЖ әзірленбейтін жаңашыл шешімдер (мысалы, білім базасында әзірге жағдай үшін үлгі жоқ); типтік сценарийлерге негізделген шешімдер, яғни белгілі шешімдермен аналогияны қолдану. «АОБ қорғау тарабының ресурстарын ұтымды бөлу процесінде қабылданатын шешімдерді қалыптастыру» кіші жүйесі мынадай жүйелілікке сәйкес көптеген шешімдерді қалыптастыруды қамтамасыз етеді:

1) математикалық модельдерді немесе сараптамалық әдістерді пайдалана отырып, шешімдер жиынын генерациялау;

2) балама шешімдерді құрылымдау;

3) баламаларды талдау кезеңінде одан әрі өңдеу және АОБ-ты қорғау тарапының ресурстарын ұтымды бөлудің ұтымды стратегиясын іздеу барысында үздік шешімдерді таңдау үшін баламалы шешімдердің түпкілікті жиынтығын қалыптастыру.

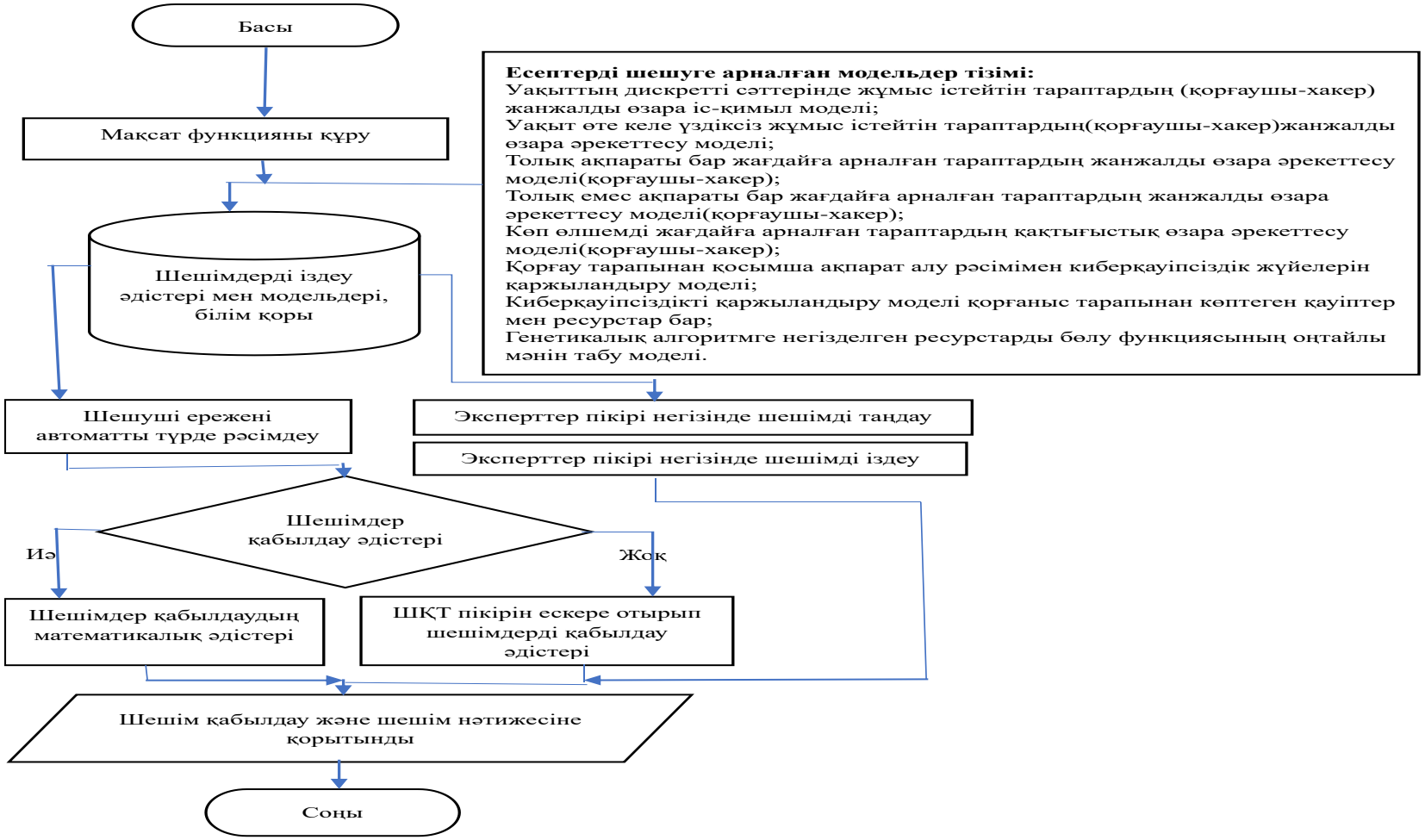
«АОБ қорғаныс жағының ресурстарын ұтымды бөлудің ұтымды стратегиясын іздеу барысында шешуші ережені қалыптастыру және баламаларды талдау» ішкі жүйесі, функционалдық әрекеттердің келесі тізбегін ұсынады, 5-суретті қараңыз,:

1) есептің шарттары бойынша шешімді таңдау үшін шешуші ережені қалыптастыру. Шешуші ережені қалыптастыру автоматтандырылған режимде немесе сарапшылар тобын тарта отырып жүргізіледі. Соңғы жағдайда, бұл – бұрын құрылған критерийтар жүйесі үшін шешілетін есепке байланысты шешуші функцияны қалыптастыратын сарапшылар. Шешуші ережені қалыптастырудың негізі критерийтардың иерархиялық құрылымдары үшін көп критерийліартықшылық функциясы болып табылады. Сондай-ақ, шешуші ереже үшін АОБ қорғаныс жағының ресурстарын ұтымды бөлудің ұтымды стратегиясын таңдауға ықпал ететін шешімдерді қолдаудың математикалық және эвристикалық ережелері маңызды;

2) қалыптасқан шешуші функция негізінде неғұрлым тиімді шешімді таңдау. АОБ-ты қорғау тарапының ресурстарын ұтымды бөлудің ұтымды стратегиясын іздеу барысында баламаларды талдау және таңдау қалыптасқан шешуші ереже негізінде жүзеге асырылады. Шешім болмаған жағдайда, ішкі жүйеде шешім нұсқаларына сараптамалық бағалау жүргізу мүмкіндігі қарастырылған. Мұны АОБ КҚ қамтамасыз етудің есебі-бағдарлама саласына сарапшыларды тарту арқылы жасауға болады.

Шешуші ережені қалыптастыру АОБ-ты қорғау тарабының ресурстарын ұтымды бөлу стратегиясын бағалау барысында туындайтын түрлі жағдайларға байланысты қалыптасқан ББ, ережелер базасы негізінде сараптамалық жүйемен бірлесіп жүзеге асырылады.

Мақсатты функцияны сараптамалық қалыптастыру сарапшылар мен ШҚҚЖ-ның өзара іс-қимылын ұйымдастыру арқылы олардың пікірлерін ББ-ға енгізу негізінде іске асырылады [89].



4.5-сурет – «АОБ қорғау тарабының ресурстарын ұтымды бөлудің стратегиясын іздеу барысында шешуші ережені қалыптастыру және баламаларды талдау» кіші жүйесінің блок-схемасы

«АОБ қорғау жағының ресурстарын ұтымды бөлудің стратегиясын іздеу барысында шешуші ережені қалыптастыру және баламаларды талдау» ішкі жүйесі шешуші функцияны автоматтандырылған режимде де, сараптамалық пікірлерді есепке алу негізінде де құруға мүмкіндік береді. Ережелерді тәуелсіз қолдану бастапқы шешімдерді және олардың осы ішкі жүйенің жұмыс істеуі нәтижесінде алынған шешімдерді салыстыруға мүмкіндік береді.

ШҚҚЖ сараптамалық кіші жүйесі жасанды интеллекттің негізгі қосымшаларының бірі болып табылады және ББ-да сақталатын нақты пәндік салаға қатысты есептерді шешуге арналған.

АОБ қорғау тарабының ресурстарын ұтымды бөлудің ұтымды стратегиясын іздеу үшін ШҚҚЖ негізі ретінде сараптамалық кіші жүйенің негізгі мақсаты бұрын [89] сипатталған модельдер негізінде әртүрлі есептерді шешуге бағдарлау болып табылады.

Сараптамалық ішкі жүйенің жұмыс істеу алгоритмінің блок-схемасы 4.6-суретте көрсетілген.

Сараптамалық ішкі жүйе сарапшы мамандардан алынған білім есебінен пайдаланушының АОБ-ты қорғау тарабының ресурстарын ұтымды бөлу стратегиясының ықтимал баламаларын әзірлеуді және бағалауды қамтамасыз етеді.

Сараптамалық ішкі жүйе мыналардан тұрады:

Есепті шешу барысында жинақталған бастапқы және аралық фактілерді сақтауға арналған ББ. Сондай-ақ, модельдер мен модельдерді басқару ережелері ББ-де сақталады. Сондай-ақ, егер АОБ қорғаныс жағының ресурстарын ұтымды бөлудің ұтымды стратегиясын таңдау есебін шешу барысында қолданылатын ережелер көп болса, ережелердің жеке базасын жобалауға болады;

АОБ қорғау жағының ресурстарын ұтымды бөлудің ұтымды стратегиясын таңдаумен байланысты есептерді шешу блогы. Бұл блок МБ және ББ-да сақталатын өлшемдер мен қағидалар негізінде АОБ-ты қорғау тарабының ресурстарын ұтымды бөлудің нақты есебін шешу үшін ережелерді орындау кезектілігінің іске асырылуын қамтамасыз етеді;

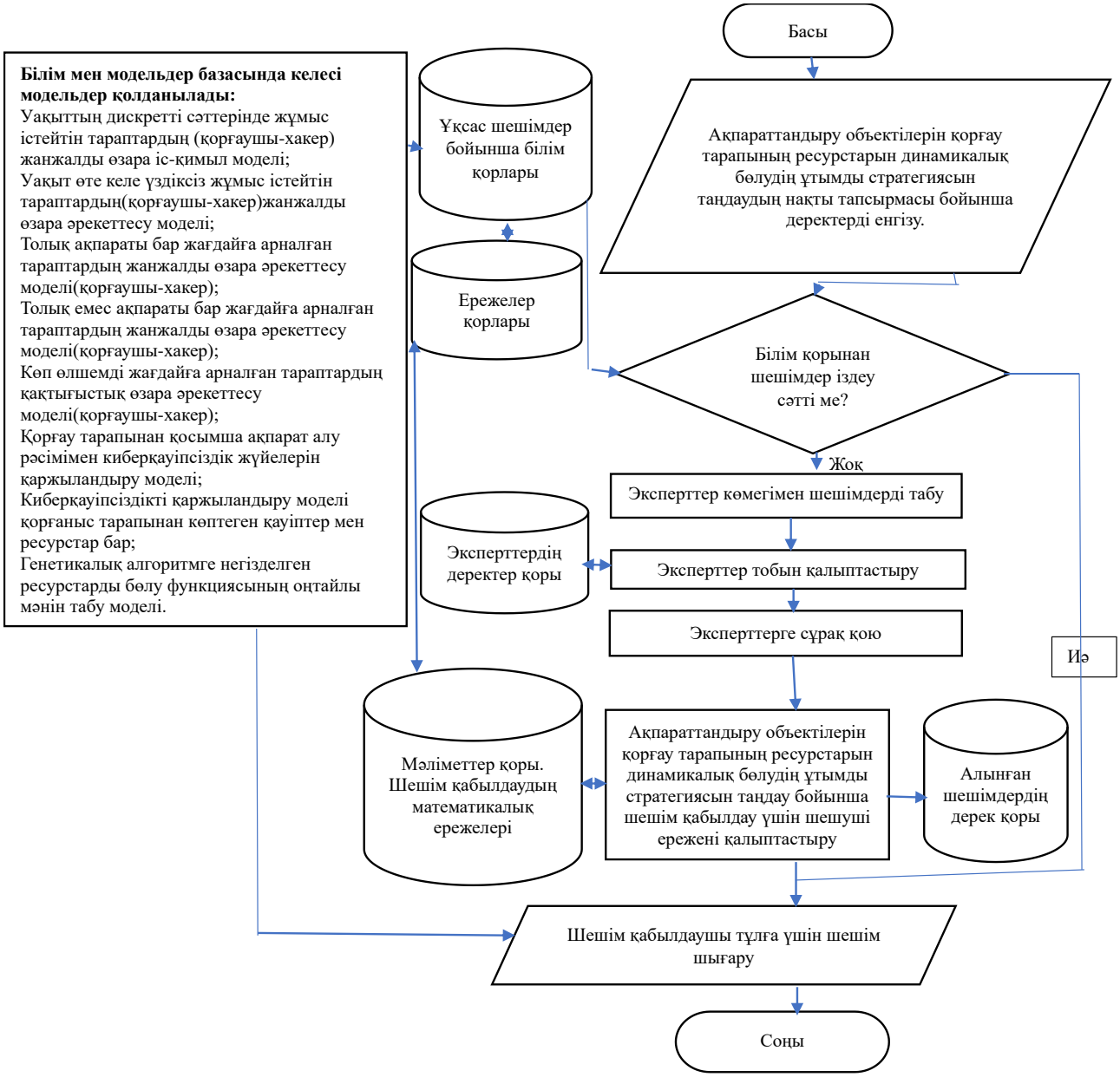
ШҚҚЖ ұсынатын ШҚТ мұндай шешімнің себебін түсінуге мүмкіндік беретін түсініктеменің ішкі жүйесі;

ББ-ге жаңа ережелер қосуға және/немесе оларды өзгертуге арналған ережелерді қалыптастыру модулі;

жалпы алғанда, пайдаланушының ішкі жүйемен және ШҚҚЖ-мен ыңғайлы диалогын жүзеге асыруға арналған диалогтық интерфейс.

4.6-суретте көрсетілген алгоритмнің жұмыс істеу әрекеттерінің реттілігі келесідей.

Тапсырмалар туралы ақпарат алған кезде шешім қолданыстағы ББ-де ізделеді. Егер осыған ұқсас жағдай бұрын кездесіп, шешім қабылдау ережелері анықталса, онда шешім осы есеп бойынша нақты анықталады.



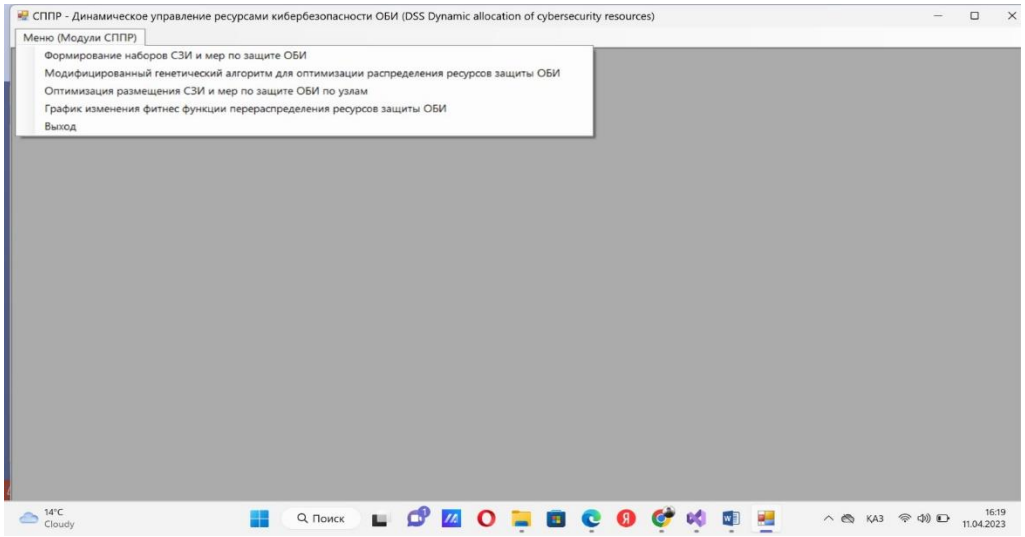
Білім мен модельдер базасында келесі модельдер қолданылады:
Уақыттың дискретті сәттерінде жұмыс істейтін тараптардың (қорғаушы-хакер) жанжалды өзара іс-қимыл моделі;
Уақыт өте келе үздіксіз жұмыс істейтін тараптардың(қорғаушы-хакер)жанжалды өзара әрекеттесу моделі;
Толық ақпараты бар жағдайға арналған тараптардың жанжалды өзара әрекеттесу моделі(қорғаушы-хакер);
Толық емес ақпараты бар жағдайға арналған тараптардың жанжалды өзара әрекеттесу моделі(қорғаушы-хакер);
Көп өлшемді жағдайға арналған тараптардың қақтығыстық өзара әрекеттесу моделі(қорғаушы-хакер);
Қорғау тарапынан қосымша ақпарат алу рәсімімен киберқауіпсіздік жүйелерін қаржыландыру моделі;
Киберқауіпсіздікті қаржыландыру моделі қорғаныс тарапынан көптеген қауіптер мен ресурстар бар;
Генетикалық алгоритмге негізделген ресурстарды бөлу функциясының оңтайлы мәнін табу моделі.

4.6-сурет – Жобаланатын ШҚҚЖ үшін сараптамалық кіші жүйенің жұмыс істеу алгоритмінің блок-схемасы

Егер есепті бастапқы қоюға шешім болмаса, онда есеплік-бағытталған сарапшылар тобы құрылады. Әрі қарай сарапшыларға жаңа шешуші ережені қалыптастыруға көмектесетін сұрақтар жіберіледі. Сарапшылар ең жақсы балама және тиісті ШҚҚЖ ішкі жүйесін таңдау үшін шешуші ереже қалыптастырады. Келесі кезеңде ең жақсы шешімді таңдау анықталады. Шешім есептің бастапқы тұжырымына сәйкес келген жағдайда ереже ережелер базасында, ал шешім ББ-де жазылады. ШҚҚЖ (немесе ЭЖ) жұмыс істеуінің осы алгоритмі АОБ қорғау тарабының ресурстарын ұтымды бөлу стратегиясын таңдаумен байланысты кез келген есеп үшін талдау және шешімді табу мүмкіндігін қамтамасыз етеді.

4.2. АОБ-ты қорғау тарабының ресурстарын ұтымды бөлудің стратегияларын іздеу барысында ШҚҚЖ модульдерін бағдарламалық іске асыру

Әзірлеген «DSS DYNAMIC ALLOCATION OF CYBER SECURITY RESOURCES» ШҚҚЖ бірнеше кіші жүйелерден тұрады. Жоғарыда көрсетілгендей, жаңа модульдерді ШҚҚЖ өзегіне қосудың орындылығына байланысты оның архитектурасы модульдік принцип бойынша құрылған. Мұндай «DSS Dynamic allocation of cyber security resources» ШҚҚЖ архитектурасы оны айтарлықтай икемді іске асыруға мүмкіндік береді, мысалы, жаңа модульдерді жазу шамасына қарай қолданыстағы модульдердің функционалына әсер етпей, оларды бас модульге қосуға болады. Осылайша, пайдаланушы тарапта (АОБ үшін ақпаратты қорғау тарабы) қажет болған жағдайда ШҚҚЖ бастапқы архитектурасын жаңа функционалдық модульдермен толықтыруға мүмкіндік бар. «DSS Dynamic allocation of cyber security resources» ШҚҚЖ бағдарламалық іске асыру қосымшаның MDI стилінде орындалған, 4.7-суретті қараңыз. Осылайша, сарапшылар бір уақытта барлық «DSS Dynamic allocation of cyber security resources» модульдерімен жұмыс істей алады.



4.7-сурет– «DSS Dynamic allocation of cyber security resources» негізгі терезесінің жалпы көрінісі

Файл мәзірінің тармағында диссертациялық зерттеу барысында іске асырылған ШҚҚЖ модульдері келтірілген. Қазіргі кезде бағдарламалық түрде [92] мынадай ШҚҚЖ модульдері іске асырылды:

1-модуль – АОБ үшін АҚҚ жинақтарын және қорғау әдістерін қалыптастыру;

2-модуль – АОБ қорғау ресурстарын бөлуді ұтымды шешуге арналған генетикалық алгоритм (диссертацияның 2-1 және 3-тарауларында ұсынылған модельдер негізінде);

3-модуль – АҚҚ орналастыруды және түйіндер бойынша АОБ қорғау жөніндегі шараларды ұтымды шешу (диссертацияның 2-тарауында ұсынылған модельдер негізінде);

4-модуль – АОБ қорғаныс ресурстарын қайта бөлу функциясын өзгерту кестесі.

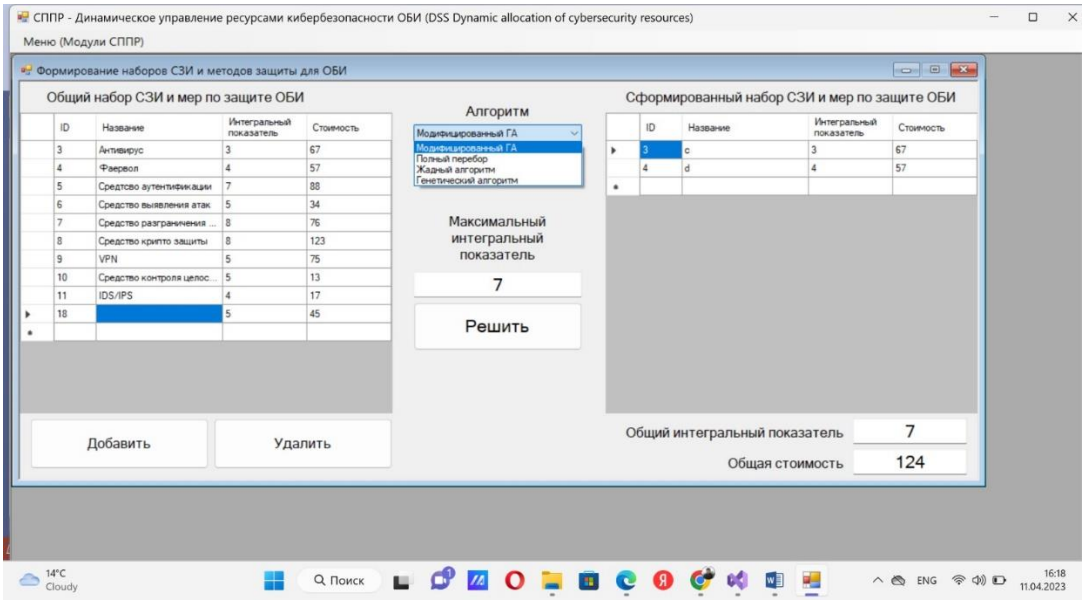
Бұл модульдердің мақсаты мен сипаттамасы төменде келтірілген.

«DSS Dynamic allocation of cyber security resources» ШҚҚЖ сарапшысының жұмысы «АОБ үшін АҚҚ жиынтығы мен қорғау әдістерін қалыптастыру» бірінші модулінен басталады. Бұл модуль интерфейсінің жалпы көрінісі төменде 4.8-суретте көрсетілген.

Сол жақта мәліметтер базасынан деректерді визуализациялау интерфейсі көрсетілген (Accessilimssqlserver), онда белгілі бір ақпараттандыру объектісінің ерекшелігіне сүйене отырып, ақпаратты қорғау құралдары мен шараларының нұсқалары бар.

Әрбір АОБ үшін негізгі шаралар мен құралдар кәсіпорындағы ақпараттық массивтердің құнына байланысты ерекшеленуі мүмкін.

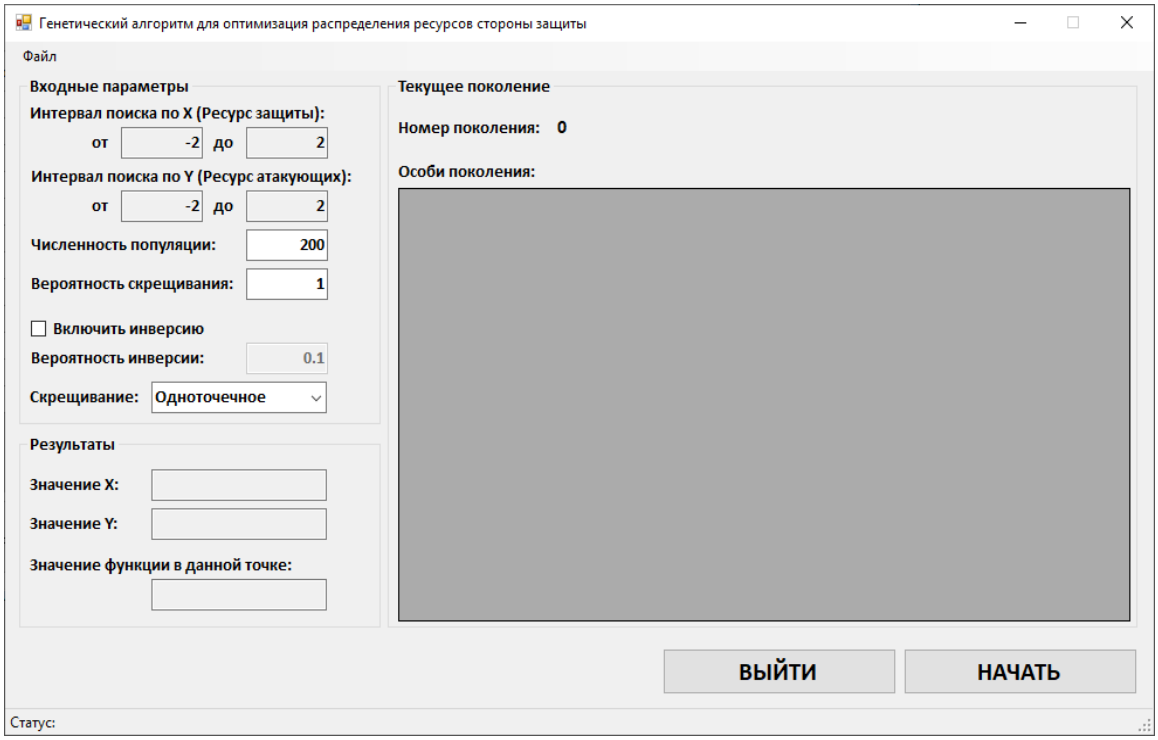
Оң жақта ұсынылған шаралар мен ақпаратты қорғау құралдарын таңдау нәтижелері бар интерфейс көрсетілген. Бұл жағдайда екі алгоритмді таңдауға болады: қарапайым сұрыптау (i7 процессоры үшін шамамен 30 минут уақыт қажет) немесе модификацияланған ГА (жұмсалған уақыт i7 процессоры үшін 1 минуттан аспады).



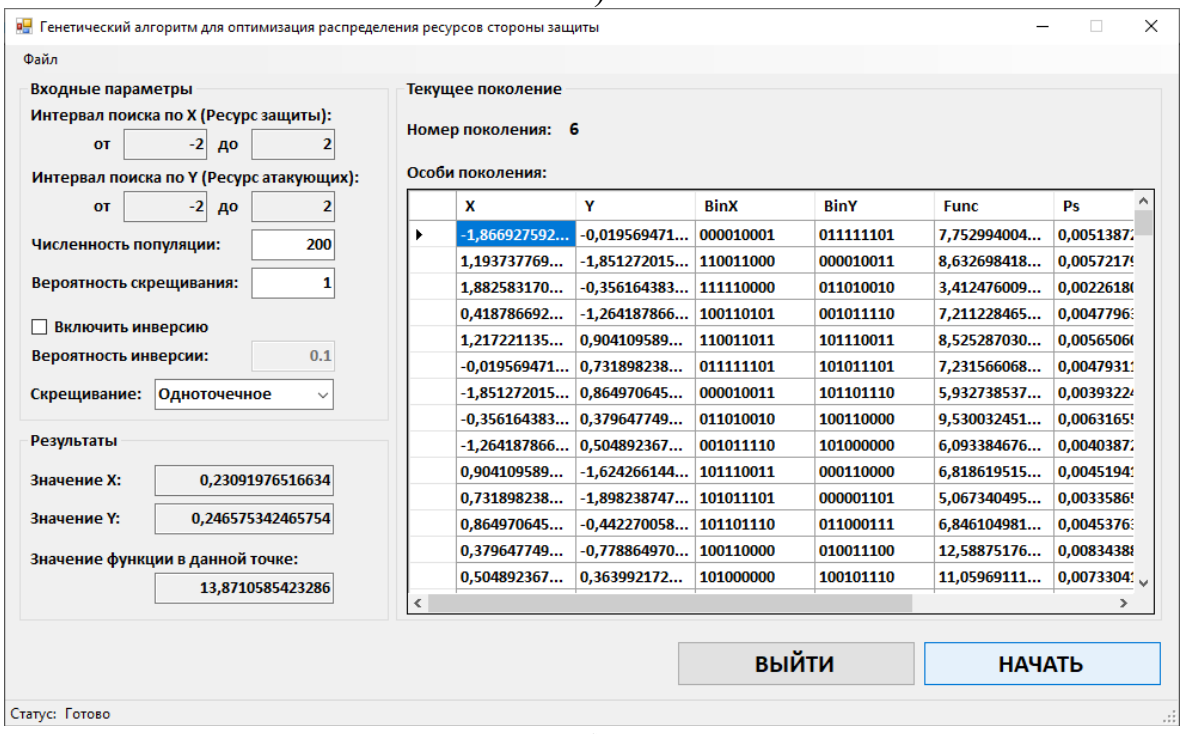
4.8-сурет– Модульдің жалпы көрінісі 1 – АОБ үшін АҚҚ жиынтығы мен қорғау әдістерін қалыптастыру

Әрі қарай, 2-модульді (4.9-суретті қараңыз) – АОБ қорғау ресурстарын бөлуді ұтымды шешудің генетикалық алгоритмін пайдалана отырып, қауіптерді жүзеге асыру нәтижесінде келтірілген залалды және АОБ объектілерінда ақпараттық ресурстарының осалдығын сипаттайтын модельдің мақсатты функциясын зерттеуге болады. Функцияның толық сипаттамасы жұмыстың екінші тарауында берілген.

4.9-суретте а) 2 модуль интерфейсінің жалпы көрінісі көрсетілген.



а)



б)

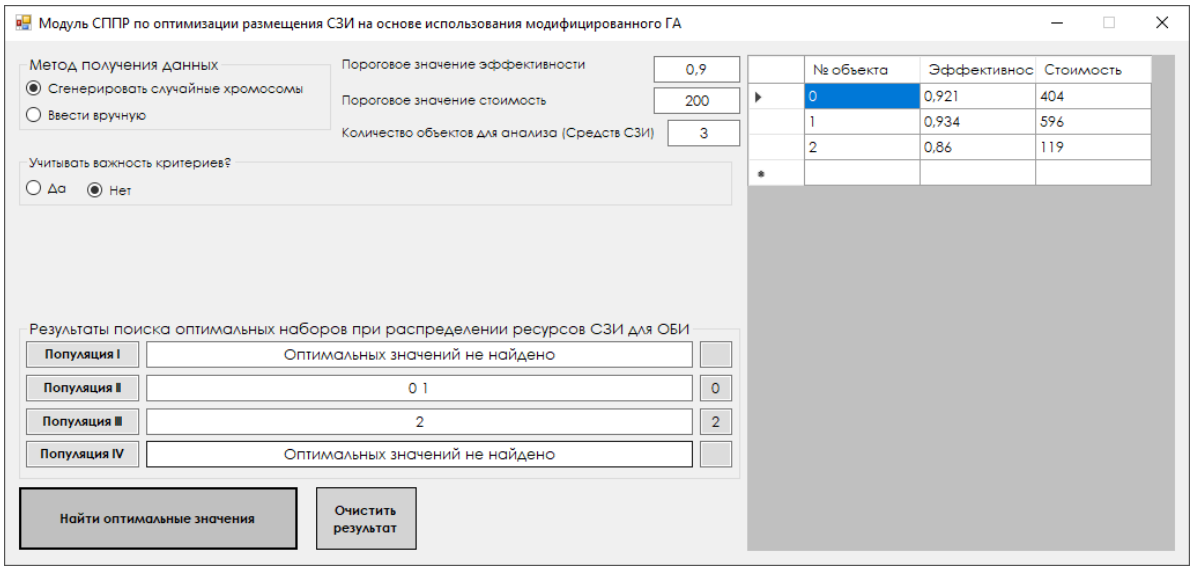
4.9-сурет – 2 модульдің жалпы түрі – АОБ қорғау ресурстарын бөлуді ұтымды шешуге арналған генетикалық алгоритм

4.9 б) суретте мақсатты функцияға кіретін және АОБ-та ақпаратты қорғауды қамтамасыз ету жөніндегі жұмыстар тізбесіне тәуелді ұтымды параметрлерді (бұл параметрлер АОБ үшін АҚҚ-ға арналған шығындардың өнімділігіне сәйкес келеді немесе жалпы жағдайда нақты АҚҚ-ның ұтымдылық көрсеткіштері мен оларды сатып алуға, қызмет көрсетуге, жаңғыртуға арналған шығындар көрсеткіштерінің арақатынасы) іздеу есебін шешудің мысалы көрсетілген (атап айтқанда, кешенді АҚҚ жобалау, әзірлеу және өрістету, АҚ (АҚОЖ) қамтамасыз ету жүйесін жетілдіру және т. б.).

Модификацияланған ГА-да қолданыстағыларға қарағанда, анық емес қатынастармен кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді ұтымды шешудің көп критерийліесебін шешу үшін Беллман-Заде қағидаты қолданылды [90]. Бұл АОБ құрамындағы компоненттердің осалдықтарын төмендетуге бағытталған іс-шаралармен байланысты жұмыстарға ресурстарды бөлуді ұтымды шешуге және шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда АОБ қорғанысының берілген мәндеріне қол жеткізуді қамтамасыз ететін ресурстар көлемінің әртүрлі нұсқаларын модельдеуге мүмкіндік берді.

Әрі қарай, сарапшы 3-модульді – АҚҚ орналастыруды ұтымды шешу және түйіндер бойынша АОБ қорғау шаралары – іске қосуы керек.

3-модульдің жалпы көрінісі 4.10-суретте көрсетілген.



4.10-сурет – 3-модульдің жалпы түрі – түйіндерде АОБ-ны қорғау бойынша АҚҚ-ны орналастыруды ұтымды шешу

3-модульде АОБ ақпараттық-коммуникациялық жүйелерінің қауіпсіздік контурлары үшін АҚҚ конфигурацияларының нұсқаларын іріктеумен және ұтымды шешумен байланысты есепті шешу үшін ГА модификациясы бағдарламалық түрде іске асырылған. Модификацияланған ГА-да (жұмыстың 3-тарауында сипатталған) АҚҚ құрамын ұтымды шешу үшін критерийтар ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасы,

АҚҚ-ның интегралдық көрсеткіштері, сондай-ақ АҚҚ-ның әрбір класы үшін құндық көрсеткіштері пайдаланылды.

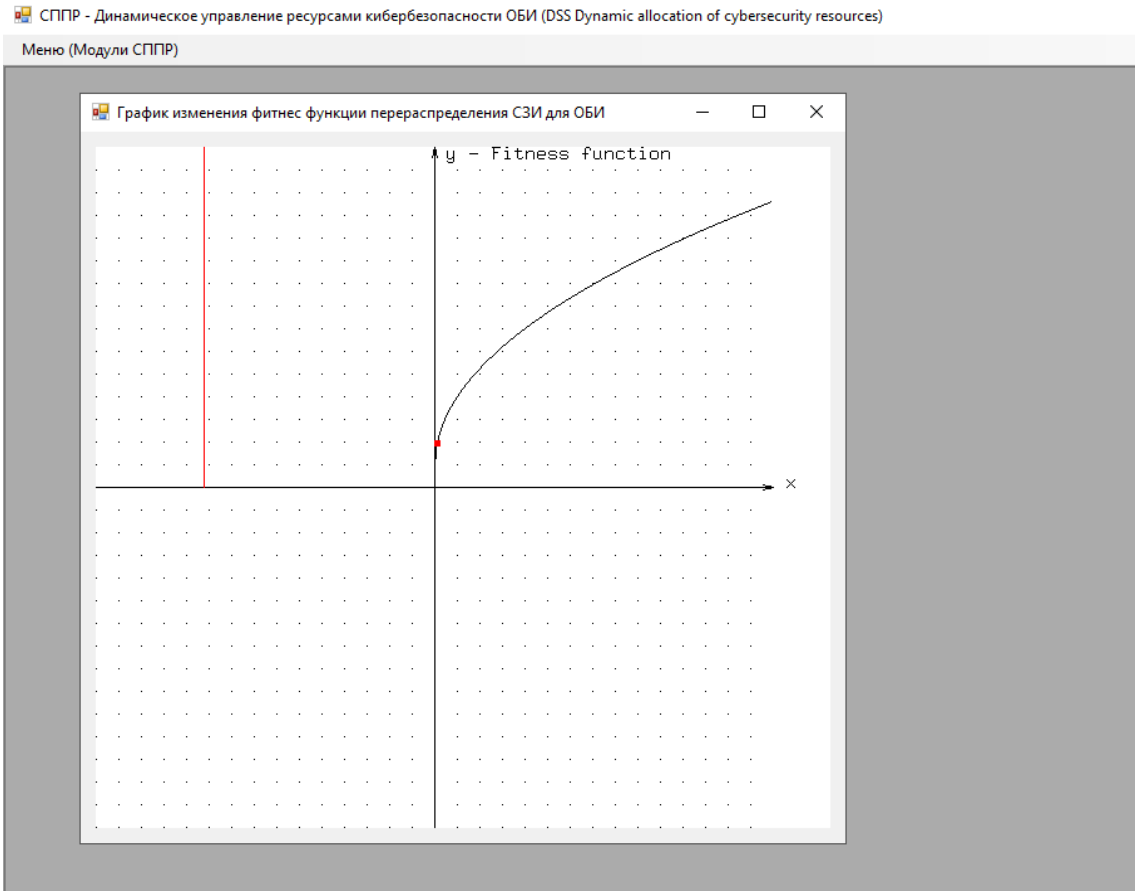
2 және 3 модульдерде АКЖ-ге арналған АҚҚ құрамын таңдауды ұтымды шешу есебінде модификацияланған ГА көп таңдаумен байланысты есептің вариациясы ретінде қарастырылады. Бұл жағдайда белгілі бір ақпараттандыру объектісі үшін АКЖ қорғаныс контурлары бойынша АҚҚ орналастыруды ұтымды шешу рюкзактың комбинаторлық есебін өзгерту ретінде қарастырылады. Ұсынылған тәсіл АКЖ түйіндерінің әрқайсысы үшін АҚҚ жиынтығын ұтымды шешу жөніндегі көп критерийліесепті шешуге ғана емес, сонымен қатар АОБ КҚ бөлінетін ресурстардың шектеулілігі жағдайында қорғау тарабының ресурстарын қайта бөлудің орындылығына жедел талдау жүргізуге мүмкіндік береді.

4.11 А) және б) суреттерде 4-модуль жұмысының мысалдары көрсетілген - АОБ қорғаныс ресурстарын қайта бөлу функциясының икемделу өзгеру кестесі.

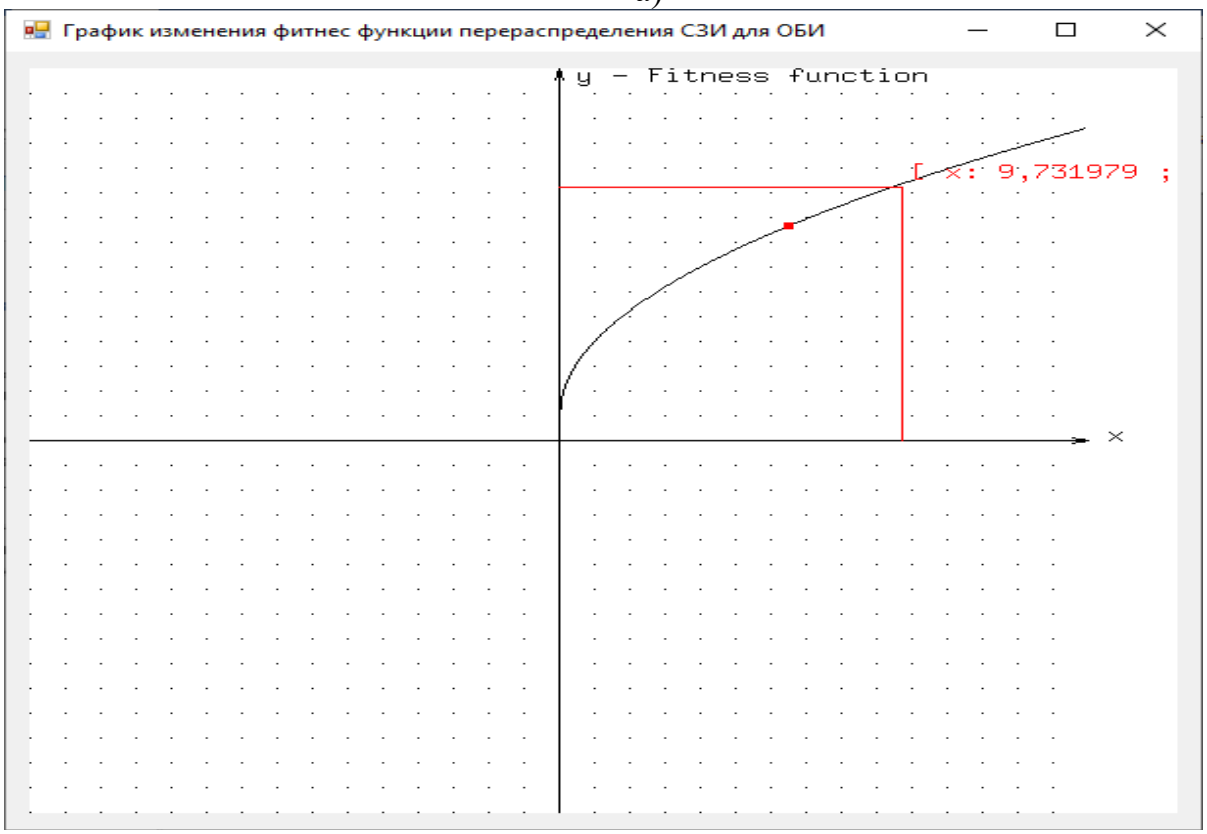
Графиктердегі қызыл нүктенің қозғалысы ГА кезінде ұрпақтардың итерациясының өзгеруін көрсетеді. Уақыт шкаласы шартты бірліктерде ұсынылған (мысалы, минут немесе он минут, өйткені әртүрлі процессорлары бар компьютерді қолданған кезде есепті шешу уақыты дұрыс болмауы мүмкін).

«DSS Dynamic allocation of cyber security resources» ШҚҚЖ тестілеу барысында ақпараттандыру объектілерінің АКЖ үшін КҚ құралдарын орналастырудың ұтымды нұсқаларын таңдау бойынша есептеу эксперименттері орындалды («Спецавтоматика в приложении» ЖШҚ үшін енгізу туралы акт). Бұл, атап айтқанда, шектеулі жағдайларда қорғаныс ресурстарын қайта бөлу есебін шешу үшін қажет. Осы «DSS Dynamic allocation of cyber security resources» ШҚҚЖ қолдану аппараттық-бағдарламалық АҚҚ және олардың АКЖ-ға арналған комбинацияларының әртүрлі нұсқаларын жылдам сұрыптауды орындауға ғана емес, сонымен бірге олардың ерекшелігіне қарай, АОБ үшін АКЖ киберқауіпсіздік контурларының құрамын ұтымды шешу бойынша қолда бар модельдермен және алгоритмдермен келтірілген модельдер мен алгоритмдерді біріктіруге мүмкіндік береді. Модельдер мен алгоритмдердің мұндай бірігуі АКЖ қорғанысын тез қалпына келтіруге мүмкіндік береді.

Сондай-ақ, диссертацияның 4-тарауында өткізілген «DSS Dynamic allocation of cyber security resources» мүмкіндіктерінің практикалық құндылығы ақпаратты жоғалтудан, АҚҚ көрсеткіштері, сондай-ақ АҚҚ-ның әрбір класы үшін құндық көрсеткіштерден туындайтын тәуекелдердің жиынтық шамасын ескере отырып, ұсынылған ГА негізінде ШҚҚЖ үшін есептеуіш ядро үшін ШҚҚЖ функционалының кеңеюіне қарай оның архитектурасына ұтымды қосылатын кітапханаларды қосу мүмкіндігімен ашық көп модульді ШҚҚЖ архитектурасын бағдарламалық іске асырудың нәтижелілігін растады.

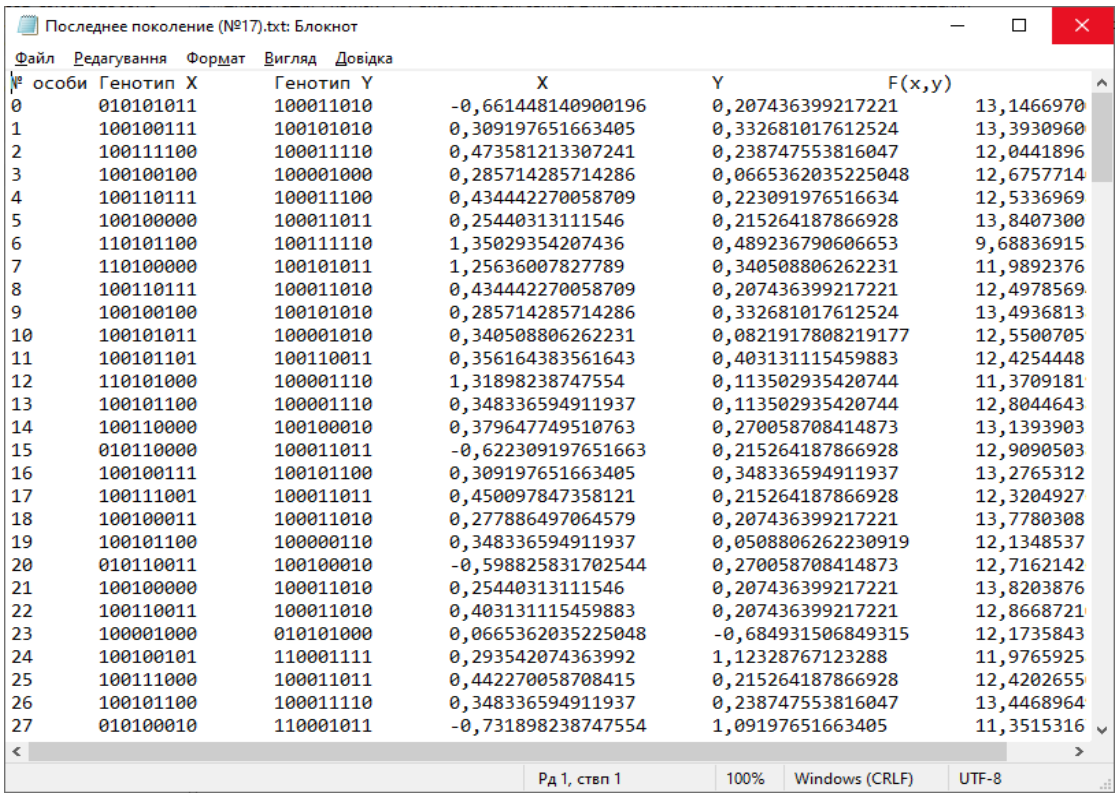


а)



б)

4.11-сурет – 4 модульдің жалпы көрінісі –АОБ қорғау ресурстарын қайта бөлу икемделу функциясын өзгерту кестесі



Последнее поколение (№17).txt: Блокнот

Файл Редагування Формат Вигляд Довідка

№ особи	Генотип X	Генотип Y	X	Y	F(x,y)
0	010101011	100011010	-0,661448140900196	0,207436399217221	13,1466970
1	100100111	100101010	0,309197651663405	0,332681017612524	13,3930960
2	100111100	100011110	0,473581213307241	0,238747553816047	12,0441896
3	100100100	100001000	0,285714285714286	0,0665362035225048	12,6757714
4	100110111	100011100	0,434442270058709	0,223091976516634	12,5336969
5	100100000	100011011	0,25440313111546	0,215264187866928	13,8407300
6	110101100	100111110	1,35029354207436	0,489236790606653	9,68836915
7	110100000	100101011	1,25636007827789	0,340508806262231	11,9892376
8	100110111	100011010	0,434442270058709	0,207436399217221	12,4978569
9	100100100	100101010	0,285714285714286	0,332681017612524	13,4936813
10	100101011	100001010	0,340508806262231	0,0821917808219177	12,5500705
11	100101101	100110011	0,356164383561643	0,403131115459883	12,4254448
12	110101000	100001110	1,31898238747554	0,113502935420744	11,3709181
13	100101100	100001110	0,348336594911937	0,113502935420744	12,8044643
14	100110000	100100010	0,379647749510763	0,270058708414873	13,1393903
15	010110000	100011011	-0,622309197651663	0,215264187866928	12,9090503
16	100100111	100101100	0,309197651663405	0,348336594911937	13,2765312
17	100111001	100011011	0,450097847358121	0,215264187866928	12,3204927
18	100100011	100011010	0,277886497064579	0,207436399217221	13,7780308
19	100101100	100000110	0,348336594911937	0,0508806262230919	12,1348537
20	010110011	100100010	-0,598825831702544	0,270058708414873	12,7162142
21	100100000	100011010	0,25440313111546	0,207436399217221	13,8203876
22	100110011	100011010	0,403131115459883	0,207436399217221	12,8668721
23	100001000	010101000	0,0665362035225048	-0,684931506849315	12,1735843
24	100100101	110001111	0,293542074363992	1,12328767123288	11,9765925
25	100111000	100011011	0,442270058708415	0,215264187866928	12,4202655
26	100101100	100011110	0,348336594911937	0,238747553816047	13,4468964
27	010100010	110001011	-0,731898238747554	1,09197651663405	11,3515316

Рд 1, ствп 1 | 100% | Windows (CRLF) | UTF-8

4.12-сурет – ШҚҚЖ мақсатты функциясы нәтижелерін шығарудың мысалы

Тарау шеңберінде жүргізілген есептеу эксперименттері шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда АОБ-ты қорғау тарапының ресурстарын бөлуді ұтымды шешуге мүмкіндік берді.

«DSS Dynamic allocation of cyber security resources» ШҚҚЖ модулін бағдарламалық іске асыру кодтарының негізгі фрагменттері қосымшада келтірілген.

4.3. 4-тарау бойынша қорытындылар

Диссертацияның соңғы тарауында келесі негізгі нәтижелер алынды:

қарсы әрекет етуші тараппен (хакермен) ұтымды қарсы тұру жағдайында ақпараттандыру объектілерінде ақпаратты қорғау тарапының ресурстарын бөлу стратегиясының ұтымды (ұтымды) нұсқасын талдау және таңдау процесінде ШҚҚЖ жұмыс істеуінің құрылымдық схемасы ұсынылды;

жүйенің үздіксіз және тиімді жұмыс істеуін қамтамасыз етуге ықпал ететін мұндай ШҚҚЖ-ның негізгі функционалдық модульдері қарастырылды. Осы ШҚҚЖ мынадай негізгі кіші жүйелеріне арналған егжей-тегжейлі блок-схемалар келтірілген: есепті, тәуекелдер мен қатерлерді талдаудың кіші жүйесі, қарсы іс-қимыл жасайтын тараппен (хакермен) ұтымды қарсы тұру жағдайында АОБ-да ақпаратты қорғау тарабының ресурстарын бөлудің болмауына байланысты; АОБ-ны қорғау ресурстарын қайта бөлу нәтижелілігін бағалаудың мақсаттары мен критерийлерін қалыптастырудың кіші жүйесі; шешімдерді қалыптастырудың кіші жүйесі; қарсы әрекет ететін тараппен ұтымды қарсы тұру

жағдайында АОБ-да ақпаратты қорғау тарабының ресурстарын бөлудің шешуші ережесін қалыптастыру және балама стратегияларын талдаудың кіші жүйесі;

келтірілген схема шағын компаниялардан немесе кәсіпорындардан бастап ірі АОБ-ға дейінгі кез келген ауқымдағы АОБ үшін қарсы әрекет етуші тараппен (хакермен) ұтымды қарсы тұру жағдайында ақпараттандыру объектілерінде ақпаратты қорғау тарабының ресурстарын бөлудің ұтымды стратегияларын таңдау процесінде шешімдердің толық функционалды қабылдануын қамтамасыз ететіндігі көрсетілген;

бірнеше ішкі жүйелерден тұратын «DSS Dynamic allocation of cyber security resources» ШҚҚЖ әзірленді. «DSS Dynamic allocation of cyber security resources» ШҚҚЖ архитектурасы модульдік принцип бойынша құрылған және бұл оны жеткілікті икемді іске асыруға мүмкіндік береді. Жаңа модульдер әзірленетіндіктен, оларды бар модульдердің функционалдық мүмкіндіктеріне әсер етпестен негізгі модульге қосуға болады. «DSS Dynamic allocation of cyber security resources» ШҚҚЖ бағдарламалық іске асыруы MDI қосымшалар стилінде орындалған;

пайдаланушы тараптың (АОБ үшін ақпаратты қорғау тарабы) қажет болған жағдайда бастапқы ШҚҚЖ архитектураны жаңа функционалдық модульдермен толықтыруға мүмкіндігі бар екені көрсетілген;

бағдарламалық түрде (VisualStudio 2019 бағдарламалау ортасы, бағдарламалау тілі#) мынадай ШҚҚЖ модульдері іске асырылды: 1 модуль – АОБ үшін АҚҚ жиынтығы мен қорғау әдістерін қалыптастыру; 2 модуль – АОБ қорғау ресурстарын бөлуді ұтымды шешуге арналған генетикалық алгоритм (диссертацияның 2-ші және 3-ші тарауларында ұсынылған модельдер негізінде); 3 модуль – тораптар бойынша АҚҚ орналастыру мен АОБ қорғау жөніндегі шараларды ұтымды шешу (диссертацияның 2-тарауында ұсынылған модельдер негізінде); 4 модуль – АОБ қорғау ресурстарын қайта бөлу функциясының икемделу өзгеру кестесі;

нақты ақпараттандыру объектілері үшін ШҚҚЖ модульдерін тестілеу орындалды (енгізу актілері қосымшада келтірілген). «DSS Dynamic allocation of cyber security resources» ШҚҚЖ тестілеу барысында ақпараттандыру объектілерінің АКЖ үшін КҚ құралдарын орналастырудың ұтымды нұсқаларын таңдау бойынша есептеу эксперименттері орындалды. Бұл, атап айтқанда, шектеулі жағдайларда қорғаныс ресурстарын қайта бөлу есебін шешу үшін қажет;

«DSS Dynamic allocation of cyber security resources» ШҚҚЖ қолдану аппараттық-бағдарламалық АҚҚ және олардың АКЖ-ға арналған комбинацияларының әртүрлі нұсқаларын жылдам сұрыптауды орындауға ғана емес, сонымен бірге олардың ерекшелігіне қарай АОБ үшін АКЖ киберқауіпсіздік контурларының құрамын ұтымды шешу бойынша қолда бар модельдермен және алгоритмдермен келтірілген модельдер мен алгоритмдерді біріктіруге мүмкіндік беретіні көрсетілген. Модельдер мен алгоритмдердің мұндай бірігуі АКЖ қорғанысын тез қалпына келтіруге мүмкіндік береді;

диссертацияның 4-тарауында өткізілген «DSS Dynamic allocation of cyber security resources» ШҚҚЖ мүмкіндіктерінің практикалық құндылығы

ақпараттың жоғалуынан болатын тәуекелдердің жиынтық шамасын, АҚҚ интегралды көрсеткіштерін, АҚҚ-ның әрбір сыныбы үшін құндық көрсеткіштерін, сондай-ақ, ақпаратты жоғалтудан туындайтын тәуекелдердің жиынтық шамасын ескере отырып, ұсынылған ГА негізінде ШҚҚЖ үшін есептеуіш өзек үшін оның архитектурасына ұтымды қосылатын кітапханаларды қосу мүмкіндігімен ШҚҚЖ ашық көп модульді архитектурасын бағдарламалық іске асырудың нәтижелілігін растады [91].

Тарау шеңберінде жүргізілген есептеу эксперименттері шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда АОБ-ты қорғау тарапының ресурстарын бөлуді ұтымды шешуге мүмкіндік берді.

ДИССЕРТАЦИЯ БОЙЫНША ҚОРЫТЫНДЫЛАР

Диссертацияда мұндай негізгі нәтижелер алынды және келесі тұжырымдар жасалды.

1. ISO / IEC TR 13335 сәйкес ақпараттық-коммуникациялық технологиялар сегменті ретінде АКЖ қауіпсіздігін басқару модельдері талданды. ISO/ IEC 27001: 2010 сәйкес «жоспарла - орында – тексер - әрекет ет» моделінің мазмұны ашылды. АОБ АҚ және оның АКЖ басқару құрылымы ақпараттың өмірлік циклі деңгейінде «объект - қауіп - қорғау» тұжырымдамасына және «кибернетикалық кеңістік - коммуникациялық орта - физикалық кеңістік» көп деңгейлі моделіне сәйкес талданды. Қолданыстағы АҚҚ ұтымды шешу модельдерін талдау қарастырылған модельдердің көпшілігінің мақсаты АҚ-ға жалпы шығындарды ұтымды шешу екенін көрсетті (Гордон-Леб моделі, К.Задираки моделі). Тек бір ғана модельдер ұтымды режимде АҚ (Глушак-Новиков моделі) объектілері арасында ұтымды қаражат бөлуді іздеуге бағытталған.

2. АОБ объектілерінде ақпараттық ресурстардың қауіптері мен осалдығын іске асырудан келтірілген залалды сипаттайтын модельдің мақсатты функциясын таңдау негізделген. Бөлшек-сызықтық функциялар материалдық тасымалдаушыларда сақталатын ақпараттың осалдығын сипаттайды, мұнда ақпаратты қорғауға, сондай-ақ ұйымдастырушылық және инженерлік-техникалық іс-шаралар мен қорғаныс құралдарына бөлінетін ресурстардың ұлғаюы, қорғаныс жағы ресурстарының мәндерінің бастапқы саласында монотонды, осалдықтың пропорционалды төмендеуіне және нәтижесінде - АОБ үшін зиян мөлшерін азайтуға әкеледі. Бөлшек сызықты емес функциялар кедергілерді жеңу үшін айтарлықтай ресурстар қажет болатын компьютерлік жүйелерде таратылатын ақпараттың қасиеттерін көрсететіні анықталды.

3. Алғаш рет жаңартылған генетикалық алгоритмді (ГА) қолдану ұсынылды. Жаңғыртылған ГА-да қолданыстағыларға қарағанда, анық емес қатынастармен кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді ұтымды шешудің көп критерийліесебін шешу үшін Беллман-Заде қағидаты қолданылды. Бұл АОБ құрамындағы компоненттердің осалдықтарын төмендетуге бағытталған іс-шаралармен байланысты жұмыстарға ресурстарды бөлуді ұтымды шешуге және шабуылдаушы тараптың ресурстары туралы

деректер болмаған жағдайда АОБ қорғанысының берілген мәндеріне қол жеткізуді қамтамасыз ететін ресурстар көлемінің әртүрлі нұсқаларын модельдеуге мүмкіндік береді.

4. Ақпараттық-коммуникациялық жүйелердің қауіпсіздік контурлары үшін ақпаратты қорғау құралдарының (АҚҚ) конфигурацияларының нұсқаларын іріктеумен және ұтымды шешумен байланысты есептерді шешу үшін ГА-ны дамытуды алды. Осы нәтижелердің ғылыми жаңалығы – ГА-да АҚҚ құрамын ұтымды шешу үшін критерийтар ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасын, АҚҚ интегралды көрсеткіштерін, сондай-ақ әрбір АҚҚ класы үшін құндық көрсеткіштерді пайдалану ұсынылатындығында. АКЖ-ға арналған АҚҚ құрамын таңдауды ұтымды шешу есебіндегі генетикалық алгоритм көп таңдаумен байланысты есептің вариациясы ретінде қарастырылады. Бұл өндірісте АҚҚ-ны АКЖ-қорғаныс контурлары бойынша орналастыруды ұтымды шешу рюкзактың комбинаторлық есебін өзгерту ретінде қарастырылады. Ұсынылған тәсіл АКЖ түйіндерінің әрқайсысы үшін АҚҚ жиынтығын ұтымды шешу жөніндегі көп критерийліесепті шешуге ғана емес, сонымен қатар АҚҚ КҚ бөлінетін ресурстардың шектеулілігі жағдайында қорғау тарабының ресурстарын қайта бөлудің орындылығына жедел талдау жүргізуге мүмкіндік береді. Зерттеудің осы бөлігінің практикалық құндылығы ақпаратты жоғалту, АҚҚ интегралдық көрсеткіштері, сондай-ақ АҚҚ-ның әрбір класы үшін құндық көрсеткіштері тәуекелдерінің ұсынылған модификациясы негізінде ШҚҚЖ есептеу өзегі үшін ұтымды қосылатын кітапхана түрінде модульді бағдарламалық іске асыруда болып табылады. Есептеу эксперименттері барысында модификацияланған ГА-ны іске асыру АКЖ-ға арналған КҚ құралдарын орналастырудың ұтымды нұсқаларын іздестіруді жеделдетуге, сондай-ақ қорғау ресурстарын олардың шектеулілігі жағдайында қайта бөлу жөніндегі есепті шешуге мүмкіндік беретіні анықталды. Бұл артықшылық аппараттық және бағдарламалық жасақтаманың әртүрлі нұсқаларын және олардың АКЖ-ға арналған комбинацияларын жылдам сұрыптап қана қоймай, сонымен бірге тарауда келтірілген модельдер мен алгоритмдерді АКЖ киберқауіпсіздік контурларының құрамын ұтымды шешу үшін қол жетімді модельдер мен алгоритмдермен біріктіруге мүмкіндік береді. Модельдер мен алгоритмдердің мұндай бірігуі АКЖ қорғанысын тез қалпына келтіруге мүмкіндік береді.

5. Ақпаратты қорғау тарапымен ресурстарды бөлудің ұтымды нұсқасын талдау және таңдау барысында ШҚҚЖ құрылымдық схемасы ұсынылды. Шабуыл жасайтын тараппен ұтымды қарсылысу жағдайына баса назар аударылады. Осыған ұқсас негізгі функционалдық модульдер қарастырылды. ШҚҚЖ модульдік архитектурасы жүйенің үздіксіз және тиімді жұмыс істеуін қамтамасыз етуге ықпал етеді. «DSS Dynamic allocation of cybersecurity resources» ШҚҚЖ барлық жүйеден тұрады. «DSS Dynamical location of cybersecurity resources» ШҚҚЖ әзірлеумен байланысты осы нәтижелердің практикалық құндылығы ақпаратты жоғалтудан туындайтын тәуекелдердің жиынтық шамасын, АҚҚ интегралдық көрсеткіштерін, сондай-ақ АҚҚ-ның әрбір сыныбы үшін құндық көрсеткіштерін ескере отырып, ұсынылған ГА негізінде ШҚҚЖ-ға

есептеуіш негіз үшін оның архитектурасына ұтымды қосылатын кітапханаларды қосу мүмкіндігі бар ШҚҚЖ ашық көп модульді архитектурасын бағдарламалық іске асырудың нәтижелілігін растады.

Жоғарыда келтірілген тұжырымдарға сүйене отырып, жұмыс мақсатына қол жеткізді және зерттеудің барлық жарияланған есептері шешілді деп айтуға болады.

Қолданылған әдебиеттер

1. Post G. V., Kagan A. Evaluating information security trade off : Restricting access can interfere with user tasks // Computers и Security. – 2007. – Vol.26, № 3. – P. 229-237.
2. Coull A., Yzerbyt V. Y., Castano E., Paladino M. P., Leemans V. Protecting the ingroup: Motivated allocation of cognitive resources in the presence of threatening ingroup members // Group Processes & Intergroup Relations. – 2001. –Vol.4, № 4. – P. 327-339.
3. Cappanera P., Scaparra M. P. Optimal allocation of protective resources in shortest-path networks // Transportation Science. – 2011. – Vol.45, № 1. – P.64-80.
4. Отчет за 2023 г. с результатами глобального опроса директоров по информационной безопасности // https://www.cisco.com. 08.05.2023.
5. Cisco Talos Incident: в 2022 г. угроз в сфере кибербезопасности меньше не станет. https://www.it-world.ru**.** 03.03.2022.
6. Отчет «Понимание киберугроз 2020». https://www.cloudav.ru. 05.07.2020.
7. Зегжда П. Д., Полтавцева М. А., Лаврова Д. С. Систематизация киберфизических системи оценка из безопасности // Проблемы информационной безопасности / Компьютерные системы. – Санкт-Петербург, 2017. – №2. – С. 127-138.
8. Калашников А. О., Аникина, Е. В. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний // Информация и безопасность. – 2018. – Т. 21, № 2. – С. 155-164.
9. Королев М. Информационная безопасность предприятия // Вестник Института экономики Российской академии наук. – Москва, 2010. – №4. – С. 187-191.
10. Евсеев С. П. Анализ законодательной базы к системе управления информационной безопасностью НСМЭП // Восточно-Европейский журнал передовых технологий. – 2015. – Т. 5, № 3. – С. 48-59.
11. Буренин А. Н., Легков К. Е., Оркин В. В. Управление инцидентами при обеспечении безопасности информационных подсистем автоматизированных систем управления сложными организационно-техническими объектами // Инфокоммуникационные технологии. – 2018. – Т. 16, № 1. – С. 122-131.
12. Mataracioglu T., Ozkan, S. Governing information security in conjunction with COBIT and ISO 27св 001. arXiv preprint arXiv:1108.2150. – 2011.
13. Sheikhpour R., Modiri N. An approach to map COBIT processes to ISO/IEC 27001 information security management controls // International Journal of Security and Its Applications. – 2012. – Vol.6, № 2. – P. 13-28.
14. Котенко И. В., Новикова Е. С. Методики визуального анализа в системах управления информационной безопасностью компьютерных сетей // Вопросы защиты информации. – 2013. – Т. 3. С. 33-42.
15. Баранова Е. К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. – 2015. – № 1 (9). – С. 73-79.

16. Шахалов И. Ю., Дорофеев, А. В. Основы управления информационной безопасностью современной организации // Правовая информатика. – 2013. – Т. 3. – С. 6-16.
17. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. – 2014. – Т. 4. – С. 126-133.
18. Дидрих В. Е., Дидрих И. В., Громов Ю. Ю., Ивановский М. А. Задача распределения ресурсов в сетевой информационной системе // Вестник Тамбовского государственного технического университета. – 2016. – № 22(4). – С. 541-547.
19. Лившиц И. И. Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI и ISO // Информатизация и связь. – 2013. – № 6. – С. 62-67.
20. Глухова Л. В., Губанова С. Е. Некоторые аспекты менеджмента информационной безопасности промышленных комплексов // Вестник Волжского университета им. ВН Татищева. – 2015. – № 3(34). – С. 1-10.
21. Siponen M., Willison, R. Information security management standards: Problems and solutions // Information & Management. – 2009. – Vol.46, № 5. – P. 267-270.
22. Gordon L. A., Loeb M. P., Zhou L. Investing in cybersecurity: insights from the Gordon-Loeb model // Journal of Information Security. – 2016. – Vol.7, № 2. – P. 49.
23. Gordon L. A., Loeb M. P., Zhou, L. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model // Journal of Cybersecurity. – 2020. – Vol.6, № 1. tyaa005.
24. Kramer A. D. An unobtrusive behavioral model of» gross national happiness» // In Proceedings of the SIGCHI conference on human factors in computing systems. – 2010, April. – P. 287-290.
25. Бабич М. Д., Задирака В. К., Людвиченко В. А., Сергиенко, И. В. // Об использовании резервов оптимизации вычислений в компьютерных технологиях решения задач прикладной и вычислительной математики с требуемыми значениями характеристик качества // Журнал вычислительной математики и математической физики. – 2010. – Т. 50, № 12. – С. 2285-2295.
26. Фомченкова Л. В., Леонов, А. В. Модель управления информационной безопасностью // Экономика и бизнес: теория и практика. – 2019. – № 12-3. – С. 106-109.
27. Калашников А. О., Аникина, Е. В. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (Часть 2) // Информация и безопасность. – 2018. – Т. 21, № 2. – С. 155-164.
28. Котенко И. В. Интеллектуальные механизмы управления кибербезопасностью // Труды Института системного анализа Российской академии наук. – 2009. – Т. 41. – С. 74-103.
29. Десницкий В. А., Котенко И. В. Модель защиты программного обеспечения на основе механизма «удаленного доверия» // Известия высших учебных заведений. Приборостроение. – 2008. – Т. 53, № 11.

30. Глушак В. В., Новіков, О. М. Синтез структуры системы защиты информации с использованием позиционной игры защитника и злоумышленника // Системнідослідження та інформаційнітехнології. – 2013. – № 2. – С. 89-100.
31. Глушак В. В., Новиков А. М., Новиков, А. Н. Синтез структуры системы защиты информации с использованием позиционной игры защитника и злоумышленника // Системные исследования и информационные технологии. – 2013. – № 2. – С. 89-100.
32. Скиба А. В., Архипов, О. Е. Информационные риски: модели рисков, исследование и использование // Инвестиции: практика и рпыт. – 2016. – № 1. – С. 51-60.
33. Лахно В. А., Петров А. С., Чертунина Н. Т. Исследование конфликтных потоков заявок в системах защиты информации // IEEE Journal on Selected Areas in Communications (JSAC). – 2006. – Т. 24, № 2. – С. 370-380.
34. Akhmetov B., Lakhno V., Akhmetov B., Alimseitova Z. Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity // In Proceedings of the Computational Methods in Systems and Software / Springer, Cham. – 2018, September. – P. 162-171.
35. Адилжанова С.А., Тюлепбердинова Г.А., Сакыпбекова М.Ж. Ақпараттандыру объектілерінің киберқауіпсіздік ресурстарын көп өлшемді ұтымды шешу мен динамикалық басқарудың математикалық әдістерін талдау // Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы. – №4(72). – 2020. – С. 145-148.
36. Soomro Z. A., Shah M. H., Ahmed, J. Information security management needs more holistic approach: A literature review // International Journal of Information Management. – 2016. – Vol. 36, № 2. – P. 215-225.
37. Ashenden D. Information Security management: A human challenge? // Information security technical report. – 2008. – Vol. 72, № 4. – P. 731-763.
38. Humphreys E. Information security management standards: Compliance, governance and risk management. information security technical report. – 2008. – Vol. 13, № 4. – P. 247-255.
39. Baker W. H., Wallace L. Is information security under control?: Investigating quality in information security management // IEEE Security&Privacy. – 2008. – Vol.5, № 1. – P. 36-44.
40. Кононович В., Тардаскина Т. Алгоритм распределения ресурсов информационной безопасности документальных телекоммуникаций // Прав., Нормативы. и метрол. обеспе. системы защиты информации в Украине. – 2004. – Т. 9. – С. 152-161.
41. Белов С. В., Попова Е. А., Кальнов М. В. Формализация задачи распределения ресурсов между различными функциями обеспечения защиты информации // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2012. – № 1. – С. 112–116.
42. Быков А. Ю., Шматова Е. С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов // Наука и образование. – 2015. – № 9. – С. 160–187.

43. Oh S. J., Fritz M., Schiele, B. Adversarial image perturbation for privacy protection a game theory perspective // In 2017 IEEE International Conference on Computer Vision (ICCV). – 2017, October. – P. 1491-1500.
44. Zhu Q., Rass, S. Game theory meets network security: A tutorial. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – 2018, January. – P. 2163-2165.
45. Маслова Н. А., Мовчан А. В. Использование интеллектуальных агентов при решении задач распределения ресурсов // Искусственный интеллект. – 2014. – № 3. – С. 80-89.
46. Ojamaa A., Tyugu E., &Kivimaa J. Pareto-optimal situaton analysis for selection of security measures // In MILCOM 2008-2008 IEEE Military Communications Conference. – 2008, November. – P. 1-7.
47. Turskis Z., Zavadskas E. K., Peldschus F. Multi-criteria optimization system for decision making in construction design and management // Engineering economics. – 2009. – Vol.61, № 1. – P. 7-17.
48. Rathgeb C., Breitinger F., & Busch C. Alignment-free cancelable iris biometric templates based on adaptive bloom filters // In 2013 international conference on biometrics (ICB). – 2013, June. – P. 1-8.
49. Kopel D. B. Peril or Protection-The Risks and Benefits of Handgun Prohibition / Louis U. Pub. L. Rev., 1993. – № 12. – P. 285.
50. Kotenko I., Sineshchuk Y., Saenko, I. Optimizing Secure Information Interaction in Distributed Computing Systems by the Sequential Concessions Method // In 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). – 2020, March. – P. 429-432.
51. Grabaum R., Meyer B. C. Multicriteria optimization of landscapes using GIS-based functional assessments // Landscape and urban planning. – 1998. – Vol.43, № 1-3. – P. 21-34.
52. Rajbhandari S., Hodgins S., Sanghvi H., McPherson R., Pradhan Y. V., Baqui A. H., Misoprostol Study Group. Expanding uterotonic protection following childbirth through community-based distribution of misoprostol: operations research study in Nepal // International Journal of Gynecology Obstetrics. – 2010. – Vol.108, № 3. – P. 282-288.
53. Alali M., Almogren A., Hassan M. M., Rassan,I. A., Bhuiyan M. Z. A. Improving risk assessment model of cyber security using fuzzy logic inference system // Computers & Security. – 2018. – Vol.74. – P. 323-339.
54. Jana D. K., Ghosh, R. Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security // Journal of information security and applications. – 2018. – Vol.40. – P.173-182.
55. Vinayakumar R., Soman K. P., Poornachandran, P. Applying convolutional neural network for network intrusion detection // In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). – 2017, September. – P. 1222-1228. IEEE.
56. Overbye T. J., Mao Z., Shetye K. S., Weber J. D. An interactive, extensible environment for power system simulation on the PMU time frame with a cyber security

application // In 2017 IEEE Texas Power and Energy Conference (TPEC). – 2017, February. – P. 1-6. IEEE.
57. Kusyk J., Uyar M. U., Sahin C. S. Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks // Evolutionary Intelligence. – 2018. – Vol.10, № 3-4. – P. 95-117.
58. He H., Maple C., Watson T., Tiwari A., Mehnen J., Jin Y., Gabrys B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing other computational intelligence. – 2016.
59. Abraham A., Grosan C., Chen Y. Cyber security and the evolution of intrusion detection systems // Journal of Engineering and Technology, ISSN, 0973-2632. – 2005.
60. Зейнельгабдин А. Б., Исабаева С. Б. Кибербезопасность Казахстана в период цифровой трансформации // Государственныйаудит. – 2019. – №4(45). – С. 47-55.
61. Перевозчиков А. Г., Решетов В. Ю., Лесик А. И. Многошаговое обобщение модели» нападение-оборона» // Вестник Тверского государственного университета. Серия: Прикладная математика. – 2017. – № 2. – С. 89-100.
62. Перевозчиков А. Г., Решетов В. Ю., Лесик, А. И. Неоднородная игра «нападение-оборона» на основе обобщенного принципа уравнивания // Вестник Тверского государственного университета. Серия: Прикладная математика. – 2018. – № 1. – С. 89-106.
63. Грищук Р.В. Теоретические основы моделирования процессов нападения на информацию методами теории дифференциальных игр и дифференциальных преобразований: Монография / Р.В. Грищук. - Житомир: Рута, 2010. – 280 с.
64. Грищук Р. В. Использование дифференциальных игр для оптимизации управления в системах защиты информации / Грищук Р.В., Хорошко В.А., Хохлачева Ю.Е. Современная защита информации. – 2012. – № 2. – С. 21–26.
65. Васин А.А. Теория игр и модели математической экономики. / А.А.Васин, В.В.Морозов. – М.: МАКС Пресс. – 2005. – 272 с.
66. Свиридов В. И., Моисеев, С. И. Математические модели оптимального распределения защитных ресурсов по источникам информационных угроз // Вестник Воронежского института высоких технологий. – 2019. – № 1. – С.110-112.
67. Быков А. Ю., Шматова, Е. С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов // Машиностроение и компьютерные технологии. – 2015. – № 9. – С.160-187.
68. Котенко И. В., Степашкин, М. В. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН. – 2004. – Т. 1, № 2. – С. 211-230.
69. Lakhno V., Akhmetov B., Adilzhanova S. The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources // ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory. – 2020. – С. 251–254, 9349310

70. Beketova G. S., Akhmetov B. S., Korchenko A. G., Lakhno A. V. Optimization backup model for critical important information systems // Bulletin of the national academy of sciences of the republic of Kazakhstan. – 2017. – № 5. – С. 37–44.
71. Братченко А. И., Бутусов И. В., Кобелян А. М., Романов А. А. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления // Вопросы кибербезопасности. – 2019. – № 1(29). – С. 18-23.
72. Шматко А. В., Сычев Е. В. Многокритериальный выбор систем защиты информации с помощью нечетких парных сравнений альтернатив // Системы обработки информации. – 2011. – № 3. – С. 161-164.
73. Ногин В. Д. Упрощенный вариант метода анализа иерархий на основе нелинейной свертки критериев // Журнал вычислительной математики и математической физики. – 2004. – Т. 44, № 7. – С. 1261-1270.
74. Шляпкин А. В. Метод оценки экономической эффективности подразделения по защите информации // Информационные системы и технологии: управление и безопасность. – 2014. – № 3. – С. 318-324.
75. Клевцов С. И., Клевцова А. Б., Буринов С. В. Модель параметрической качественной иерархической оценки состояния технической системы // Инженерный вестник Дона. – 2015. – Т. 37, № 3. – С. 1-18.
76. Chiba Z., Abghour N., Moussaid K., El Omri A., Rida M. New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm // International Journal of Communication Networks and Information Security. – 2019. – Vol.11, № 1. – P. 61-84.
77. Nozaki Y., Yoshikawa M. Security evaluation of ring oscillator puf against genetic algorithm based modeling attack. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. – Springer, Cham, 2019. – P. 338–347.
78. Lakhno V., Bereke M., Adilzhanova S., Desiatko A., Palaguta K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization // Journal of Theoretical and Applied Information Technology. – 2022. – Vol.100, № 7. – P. 1693-1705.
79. Sureshkumar T., Anand B., Premkumar T. Efficient Non-Dominated Multi-Objective Genetic Algorithm (NDMGA) and network security policy enforcement for Policy Space Analysis (PSA) // Computer Communications. – 2019. – Vol.138. – P. 90–97.
80. Shang Q., Chen L., Wang D., Tong R., Peng P. Evolvable Hardware Design of Digital Circuits Based on Adaptive Genetic Algorithm. In International Conference on Applications and Techniques in Cyber Security and Intelligence. – Springer, Cham, 2019. – P. 791–800.
81. Baroudi U., Bin-Yahya M., Alshammari M., &Yaqoub U. Ticket-based QoS routing optimization using genetic algorithm for WSN applications in smart grid // Journal of Ambient Intelligence and Humanized Computing. – 2019. – Vol.10, № 4. – P. 1325-1338.
82. Llansó T., McNeil M., Noteboom C. Multi-Criteria Selection of Capability-Based

Cybersecurity Solutions // In Proceedings of the 52nd Hawaii International Conference on System Sciences. – 2019. – P. 7322–7330.
83. Yan D., Liu F., Zhang Y., Jia K., Zhang Y. Characterizing the Optimal Attack Strategy Decision in Cyber Epidemic Attacks with Limited Resources // In International Conference on Science of Cyber Security. – Springer, Cham, 2018. – P. 65–80.
84. Lee Y., Choi T. J., Ahn C. W. Multi-objective evolutionary approach to select security solutions // CAAI Transactions on Intelligence Technology. – 2019. – Vol.2, № 2. – P. 64-67.
85. Lakhno V., Adilzhanova S., Kryvoruchko O., Desiatko A., Buriachok V. Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm // In: Silhavy R. (eds) Informatics and Cybernetics in Intelligent Systems / CSOC 2021. Lecture Notes in Networks and Systems, vol 228. Springer, Cham.
86. Akhmetov B., Lakhno V., Akhmetov B., Alimseitova Z. Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity // In Proceedings of the Computational Methods in Systems and Software. – Springer, Cham, 2018. – P.162–171.
87. Akhmetov B., Lakhno V., Adilzhanova S., Conceptual Diagram of An Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems // Journal of Theoretical and Applied Information Technology. – 2021. – Vol.99, № 18. – P. 4297-4310.
88. Ахметов Б.С., Адилжанова С.А., Қорғаныс объектілері арасында ресурстарды бөлуді ұтымды шешу кезінде шешім қабылдауды қолдаудың модульдік жүйесі // Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы. – 2021. – №4(76).
89. Лахно В.А., Адилжанова С.А. Генетикалық алгоритмді кибер қауіпсіздік ресурстарының динамикалық бақылау есептерінде қолдану// Вестник КазНИТУ им.Сатпаева. – 2020. – №6(142). – С. 565-568.
90. Адилжанова С.А., Ахметов Б.С., Лахно В.А., Ақпаратты қорғау тарапының ресурстарын іріктеу, ұтымды шешу және қайта бөлу есепсін шешу үшін генетикалық алгоритмді дамыту. // Вестник Алматинского университета энергетики и связи. – 2022. – № 1(56).
91. Lakhno V., Akhmetov B., Malyukov V., Kartbayev T. S. Modeling of the decision-making procedure for financing of cyber security means of cloud services by the medium of a bilinear multistep quality game with several terminal surfaces // International Journal of Electronics and Telecommunications. – 2018. – Vol.64, № 4. – P. 467-472.
92. Адилжанова С.А. Использование генетического алгоритма в задаче динамического управления ресурсами кибербезопасности. // « Международная научная конференция студентов и молодых ученых «ФАРАБИ ӘЛЕМІ», КазНУ имени аль-Фараби. – 2021. – 73 с.
93. Akhmetov B., Lakhno V., Adilzhanova S. Automation of Information Security Risk Assessment // International Journal of Electronics and Telecommunications. – 2022. – Vol.68, № 3. – P. 549-555.

ҚОСЫМША А-Авторлық куәлік

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ

РЕСПУБЛИКА КАЗАХСТАН

СВИДЕТЕЛЬСТВО

О ВНЕСЕНИИ СВЕДЕНИЙ В ГОСУДАРСТВЕННЫЙ РЕЕСТР ПРАВ НА ОБЪЕКТЫ, ОХРАНЯЕМЫЕ АВТОРСКИМ ПРАВОМ

№ 27587 от «30» июня 2022 года

Фамилия, имя, отчество, (если оно указано в документе, удостоверяющем личность) автора (ов):
АЛИЛЖАНОВА САЛТАНАТ АЛЬМУХАНБЕТОВНА, АХМЕТОВ БАХЫТЖАН СРАЖАТДИНОВИЧ, ЛАХНО ВАЛЕРИЙ АНАТОЛЬЕВИЧ

Вид объекта авторского права: **произведение науки**

Название объекта: **Программный комплекс СППР «DSS Dynamic allocation of cybersecurity resources»**

Дата создания объекта: **21.06.2022**

Құжат түпнұсқалығын http://www.kazpatent.kz/ru сайтының "Авторлық құқық" бөлімінде тексеруге болады. https://copyright.kazpatent.kz

Подлинность документа возможно проверить на сайте kazpatent.kz в разделе «Авторское право» https://copyright.kazpatent.kz

Подписано ЭЦП

Н. Абулкаиров

Қосымша Б – МГА қолдану алгоритмінің программа листингі

```
#define _USE_MATH_DEFINES
#include <iostream>
#include <cmath>
#include <ctime>
using namespace std;
double func(double x, double a)
{ return pow(x, 3) / pow(x, 3) + 8;}
doublemutation(double x0, double x1)
{
constint NUM = 100000000;
return fabs((double)((rand() * NUM) % (int)((x1 - x0) * NUM) + 1) / NUM) +
x0;
}
double inversion(double x, double eps)
{
   static int sign = 0; sign++;    sign %= 2;    if (sign == 0) return x - eps;
   else return x + eps;}
void crossover(double* x, double eps, double x0, double x1)
{
int k = 99;
   for (inti = 0; i< 8; i++)
      for (int j = i + 1; j < 8; j++)
{
         x[k] = (x[i] + x[j]) / 2;
         k--;
      }
   for (inti = 0; i< 8; i++)
   {
      x[k] = inversion(x[i], eps); k--;
      x[k] = inversion(x[i], eps); k--;
   }
   for (inti = 8; i< k; i++)
      x[i] = mutation(x0, x1);
}
void sort(double* x, double* y)
{
   for (inti = 0; i< 100; i++)
      for (int j = i + 1; j < 100; j++)
         if (fabs(y[j]) <fabs(y[i])) {
            double temp = y[i];
            y[i] = y[j]; y[j] = temp;temp = x[i];  x[i] = x[j];  x[j] = temp;    }}
double genetic(double x0, double x1, double eps)
{
```

```
double population[100];
   double f[100];
intiter = 0;
for (int i = 0; i < 100; i++)
{
      population[i] = mutation(x0, x1);
      f[i] = func(population[i], 5);
   }
sort(population, f);
   do {iter++;
crossover(population, eps, x0, x1);
      for (inti = 0; i< 100; i++)
         f[i] = func(population[i], 53);
sort(population, f);
   } while (fabs(f[0]) > eps&&iter< 20000);
cout<<iter<< " iterations" <<endl;
   return population[0];}
intmain()
{
srand(time(NULL));
cout<<genetic(1.0, 10.0, 0.000001);
cin.get();
   return 0;}
```

ҚОСЫМША В- Ғылыми зерттеу нәтижелерін енгізу актісі

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ СПЕЦАВТОМАТИКА

Код ЄДРПОУ 30278200, 02081, м. Київ, Дарницький район, ВУЛИЦЯ ЗДОЛБУНІВСЬКА, будинок 3

20/10-22

1 від 06 2022 р.

АКТ ВПРОВАДЖЕННЯ (ВИКОРИСТАННЯ)
результатів дисертаційної роботи
Адилжановой Салтанат Альмуханбетовни
на тему: «Методи, моделі та інформаційні технології для динамічного управління ресурсами кібербезпеки», представленої на здобуття ступеню доктора філософії PhD
за спеціальністю 8D06301 – «Системи інформаційної безпеки»
(м. Алмати, Казахстан)

Розроблена модульна СППР «DSS Динамічний розподіл ресурсів кібербезпеки». Програмна реалізація СППР «Динамічний розподіл ресурсів кібербезпеки DSS» виконана в стилі додатків MDI. Під час апробації СППР «DSS Dynamic allocation of cybersecurity resources» доведено, що використання СППР дозволяє виконувати швидкий перебір різних варіантів апаратно-програмних СЗІ та їх комбінації для ІКС. Підтверджена ефективність відкритої багатомодульної архітектури СППР з можливістю розширення функцій СППР шляхом додавання в її архітектуру динамічних приєднаних бібліотек для обчислювального ядра для СППР.

Головний інженер
ТОВ «Спецавтоматика» Коржук А.Г.