Абай атындағы Қазақ ұлттық педагогикалық университеті

ӘОЖ 004.02.056. 5:378 Қолжазба құқығында

ҚЫДЫРАЛИНА ЛАЗАТ МУКТАРОВНА

Жоғары оқу орнының ақпараттық білім беру ортасын кіріктірілген қорғаудың әдістері мен модельдері

6D060200 – Информатика

Философия докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

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

Қазақстан Республикасы
Алматы, 2020

МАЗМҰНЫ

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

ЖОО - жоғары оқу орны
АББО - ақпараттық білім беру ортасы
ЖОО АББО - жоғары оқу орнының ақпараттық білім беру ортасы
АКТ- ақпараттық- коммуникациялық технологиялар
АҚ - ақпараттық қауіпсіздік
КҚ – киберқауіпсіздік
АТ- ақпараттық технологиялар
АТЖ - ақпараттық технологиялар жүйелері
АКЖ-ақпараттық-коммуникациялық жүйелері
АЖ- ақпараттық жүйелер
КАЖ-корпоративтік ақпараттық жүйелер
РЕҚ-рұқсат етілмеген қолжетімділік
АҚЖ -ақпаратты қорғау жүйелері
АН- ақпараттандыру нысандары
СЖ -сараптамалық жүйелер
ГЛ - Гордон-Лоеб
АТҚ- ақпаратты техникалық қорғау
БҚ -берілгендер қоры
АҚҚ-ақпаратты қорғау құралдары
DSS- Decision Support Systems (шешімдерді қабылдауды қолдау жүйесі)
ШҚҚЖ - шешімдерді қабылдауды қолдау жүйесі
ШҚҚИЖ -шешімдерді қабылдауды қолдау интеллектуалды жүйесі
ҚР -қаржы ресурсы
ТТС- тепе –теңдесу сәулесі
ЖОО АББО АР - ЖОО АББО-ның ақпараттық ресурстары
ЫПЖ -ықтимал Петридің желілері
ПМЖ - Петри-Марков желілері
ҚББ - қолжетімділікті бақылау және басқару
ПМЖ - Петри модификацияланған желілері
ҚБЖ - қолжетімділікті басқару жүйесі
ФК - функционалдық компоненттер
РЕҚ - рұқсат етілмеген қолжетімділік
ҚДЖ – қатерді детекторлау жиынтығы
ҚДЖЖ-қатерлерді детекторлау үшін пайдаланылатын жиынтықтар жиыны
ЖҚДЖ - жаңартылатын ҚДЖ
БН - базалық нысандар
ДЖ -детекторлық жиынтық
ҚКЖ- қорғаудың кіріктірілген жүйесі

ЗН- Зерттеу нысандары
ТКҚ- техникалық күзет құралдары
ТС-техникалық сипаттамалар
ШҚЖТ-шешім қабылдауға жауапты тұлға
ҚБҚ- қолданбалы бағдарламалық қамсыздандыру
ДК -дербес компьютер
БТПҰУ- Биоресурстар және табиғатты пайдалану ұлттық университеті
ЖЕЖ - жергілікті есептеу желілері
ҚҚБӘ - қолжетімділік құқықтарын бақылау әдісі
АРТҚҚ - ақпараттық ресурстарын техникалық қорғау құралдары

КІРІСПЕ

Зерттеудің өзектілігі: Жоғары оқу орнының қызметінің дамуы мен тиімділігін арттыру саласындағы өзекті рөлдерінің бірі оның ғылым мен техниканың дамыған сайын әлемде пайда болатын жаңа тәсілдерді, технологиялар мен құралдарды үнемі іздеп, қолдануға баса назар аударатындығы болып табылады. Осыған байланысты университет жаһандық цифрландыру мен ақпараттандыру үдерістерінен, әсіресе, соңғы жылдары төртінші өнеркәсіптік революцияға қатысты технологиялар мен құралдардың жаңа түрлерін ажырату мен қалыптастыруға байланысты өзекті болып отырған үдерістерінен тыс қала алмайды. Мұндай технологиялар техникалық құралдарға адамның араласуынсыз бір-бірімен әрекеттесуіне мүмкіндік береді. Цифрлық технологияларды қолдана отырып, өмір сүруге және оқуға дайын жаңа ұрпақ қалыптастыру білім беру жүйесінің дамуына қосымша негіз болып табылады.

Осы және басқа факторларды ескерсек, уақытылы және жан-жақты цифрландыру стратегиялық сипат алып, сәйкес тұжырымдамалық тәсілдерді іздеп жүйелеуді талап етеді. Айқын мысал ретінде профессор Т.О.Балықбаев пен профессор Е.Ы.Бидайбеков басшылығымен құрылған Абай атындағы Қазақ ұлттық педагогикалық университетін цифрландыру тұжырымдамасын қарастыруға болады. Тұжырымдаманың мазмұны жоғары оқу орнының цифрлық инфрақұрылымын талдау нәтижелерін ескере отыра жасалынып, соның негізінде университетті цифрландырудың басым бағыттары айқындалған. Оқу және оқытушылық қызметті цифрландырудың теориялық және практикалық негіздері, университеттің ғылыми-зерттеу және әлемдік ғылыми қауымдастыққа кірігіуі, университеттің цифрландыруда студенттер мен оқытушылардың цифрлық құзырлылығын дамыту тәсілдері қарастырылған [1].

Тұжырымдамада университеттің цифрлық білім беру ортасының ақпараттық қауіпсіздігік және оның құрамдас бөлігі киберқауіпсіздік мәселелеріне ерекше назар аударылған. Заманауи жоғары оқу орындарында, кез келген мемлекеттің интеллектуалдық және еңбек потенциалын дамытатын көптеген педагогтар, ғылыми қызметкерлер еңбек етеді, он мыңдаған студенттер оқиды. Осыған байланысты, қазіргі жағдайда жоғары оқу орындары мен басқа да оқу орындарының ақпаратты қауіпсіздігін (АҚ) және киберқауіпсіздігін (КҚ) қамтамасыз ету міндеттері өте маңызды.

Айта кететін жағдай, жоғары оқу орындарының АҚ-ны қамтамасыз ету және КҚ-ны басқару саласында бірқатар проблемалар бар, олардың ішіндегі ең маңыздылары: ЖОО АББО-ның ақпараттық ресурстарды техникалық қорғау құралдарымен (АРТҚҚ) нашар жабдықталуы; киберқауіпсіздікті қамтамасыз ету бойынша міндеттерді шешуді қамтамасыз ететін жабдықтардың (қосқыштар, маршрутизаторлар, брандмауэр және т.б.) моральдық және физикалық тозуы; жоғары оқу орындарында IT департаменттердің штат кестелерінде ЖОО АББО-да КҚ-ны қамтамасыз етуге бөлінген мақсатты

қаржыландыруды сауатты және оңтайлы бөле алатын АҚ және КҚ міндеттеріне жауапты арнайы даярланған мамандардың болмауы.

ЖОО АББО-дағы КҚ-ны басқарудың қолданыстағы тәсілдері негізінен коммерциялық кәсіпорындарға немесе режимдік (жабық) нысандарға тән. Алайда, білім беретін мекемелер мен жоғары оқу орындарының өзіндік ерекшеліктері бар. ЖОО АББО-ның КҚ жүйесін жобалаушылар АҚ-ны басқару жүйесін құру процесінде келесі қиындықтарды атап өтеді:

– ЖОО АББО-ның АҚ-ның және КҚ-ның ағымдағы жағдайын бағалаудың арнайы әдістерінің болмауы;

– ЖОО АББО-ның қорғалатын ресурстарына деструктивті әсер етуші факторлардың белгісіздігі мен ерекшелігі;

– ЖОО АББО-ның ақпараттық ресурстарын қорғау құралдарының тиімділігін бағалау үшін пысықталған әдістер мен алгоритмдердің болмауы.

Компьютер қаскүнемдері (хакерлер) тарапынан әртүрлі компьютерлендірілген жүйелерге (мысалы, ЖОО АББО) деструктивті әсерлердің саны мен күрделілігінің өсуі жағдайында, техникалық қызмет көрсетушілердің алдында тұрған маңызды міндеттердің бірі, олардың киберқауіпсіздігін қамтамасыз ету. Бұл тиісті қаржыландыруды инвестициялауды талап етеді. ЖОО АББО-ның ақпараттық қауіпсіздігі мен киберқауіпсіздігін қаржыландыру бойынша шешім қабылдау ақпаратты сенімді қорғауды қамтамасыз етуге тән барлық факторларды ескере отырып, қаржыландыруды жүзеге асыруға мүмкіндік беретін процедураларға негізделуі тиіс.

Ақпаратты қорғау және ақпараттандырудың әртүрлі нысандардың ақпараттық қауіпсіздігі мен киберқауіпсіздігін басқарудың тиімді жүйелерін құру міндеттерімен көптеген шетелдік ғалымдар: Д.П.Зегжда [2], С.В. Казмирчук [3], В.А.Лахно [3], А.Г.Корченко [4], В.И.Котенко [5], M.Atighetchi [6], R.H.Campbel[7], J. Dawkins [8], А.С. Марков [9], M.Endler [10] айналысқан. Бұл мәселелерді зерттеуге отандық мамандар да өз үлестерін қосты: Р.Г.Бияшев [13], М.Н.Калимолдаев [13], Б.С. Ахметов[12], У.А.Тукеев [12], И.Т.Утепбергенов [14], В.В.Яворский [14], Т.С.Картбаев [11], Ж.К.Алимсеитова [11] және басқа да ғалымдар.

Ақпараттық ресурстарды техникалық қорғау құралдарын (АРТҚҚ) қаржыландыру саласында, оның ішінде ЖОО АББО-ны қаржыландыру бойынша зерттеу жұмыстарының көпшілігінде киберқауіпсіздік құралдарына және АРТҚҚ-ға қаржы ресурстарын инвестициялаудың оңтайлы стратегияларын іздеу міндеттерінің экономикалық қойылымына ғана назар аударылған. Бұл жұмыстар осыған ұқсас жобаларға бақылау және шешім қабылдау процедураларына ең озық ақпараттық технологияларды енгізу тенденцияларын, сондай-ақ өздерінің мақсаттарына жету үшін ақпараттық қауіпсіздік пен киберқауіпсіздік контурларынан өтуге тырысатын компьютер қаскүнемдерінен келетін шығындардың өсіп отырғанын ескермейді.

Сондықтан, киберқауіпсіз ЖОО АББО-ны құру мен қолдауға, жоғары оқу орындарының шектеулі қаржы ресурстарын үлестірудің оңтайлы

стратегияларын табуға мүмкіндік беретін шешімдерді қабылдауды қолдау компьютерлік интеллектуалды жүйелері үшін әдістер мен модельдерді дамыту бағытында жаңа зерттеулер қажет.

Ақпараттық қауіпсіздік және киберқауіпсіздік проблемаларына арнаған зерттеу жұмыстарында көптеген ғалымдардың зерттеулері көрсеткендей, ақпараттандырудың киберқауіпсіз нысан құрудың негізгі мүмкіндіктерімен, атап айтқанда, заманауи ақпараттық технологияларды пайдалану негізінде ЖОО АББО-ның КҚ-ны дамытудың негізгі мүмкіндіктерімен және қорғаушының жеткіліксіз қаржыландырылуы немесе рационалды емес қаржы стратегиясының салдарынан киберқауіпсіздікті тиісті деңгейде қамтамасыз ете алмайтын, қолданыстағы қорғаныс жүйелерінің тиімділігінің жеткіліксіздігі арасында айқын **қарама-қайшылық** бар.

Жоғарыда көрсетілген қарама-қайшылықты шешу үшін диссертацияда ЖОО АББО-да қорғаушының стратегияларын іздеу есебінде шешімдерді қабылдауды қолдаудың көп модульдік жүйесін құрудың модельдерін, әдістерін және ақпараттық технологияларын құрудан тұратын жаңа ғылыми міндет қойылған. Қойылған міндет ЖОО АББО-ның киберқауіпсіздігін және ақпараттық ресурстарды техникалық қорғау құралдарын инвестициялауға жұмсалатын нақты мәліметтермен болжанған мәліметтердің айырмашылығын азайтуға, сондай-ақ нақты ЖОО АББО үшін киберқауіпсіздікті және ақпараттық ресурстарды техникалық қорғау құралдарын қорғаушы тарапынан қаржыландырудың оңтайлы стратегиясын алуға мүмкіндік береді. Сондықтан, ЖОО АББО-ны қорғау стратегияларын іздеу міндеттерінде шешім қабылдауды қолдау жүйесін құрудың модельдерін, әдістерін және ақпараттық технологияларын ғылыми негіздеуге бағытталған диссертациялық жұмыстың тақырыбы өзекті және ғылыми, практикалық қызығушылық тудырады.

Зерттеудің мақсаты: шешімдерді қабылдауды қолдау жүйесін қолдана отырып, қорғаушының оңтайлы қаржы стратегияларын іздеу және ЖОО АББО-да ақпараттың құпиялылығына, тұтастығына және қолжетімділігіне деструктивті әсерлердің саны үнемі өсуі жағдайында сәйкес қарсы шаралар құру негізінде ЖОО АББО-ны қорғаудың әдістері мен модельдерін дамыту.

Зерттеудің нысаны: ЖОО АББО-да ақпаратты қорғау құралдарына және киберқауіпсіздігіне берілген ресурстарды үлестіру процестері.

Зерттеу пәні: Жоғары оқу орнының ақпараттық білім беру ортасын кіріктірілген қорғаудың әдістері мен модельдері.

Зерттеудің ғылыми болжамы: егер, ЖОО АББО-ны қорғаудың оңтайлы қаржы стратегияларын таңдау қажет болса, онда шешімдерді қабылдауды қолдау интеллектуалды жүйелерін қолдану арқылы бұл мәселені тиімді және кешенді шешуге болады. ШҚҚЖ-ның есептеу ядросы әдістер мен модельдерден тұрады, олар тәуелді қозғалыстармен берілген бисызықты көп қадамды сапа ойындар теориясына, Петри желілерінің теориясына және т.б. негізделген. Бұл әдістер мен модельдердің жиыны ЖОО АББО-ны

қорғаушының «қалау» жиынын және оңтайлы стратегияларын анықтауға мүмкіндік береді.

Зерттеу міндеттері:

– ЖОО АББО-ны қорғауды қамтамасыз ету саласындағы алдыңғы зерттеулерге шолу мен талдауды орындау және ЖОО АББО-ның киберқауіпсіздік жүйесіндегі инвестициялық процесс параметрлерінің әртүрлі қатынастарын ескере отырып, инвестициялауды басқару стратегияларын табу бойынша шешімдерді қабылдауды қолдау жүйесіне (ШҚҚЖ) арналған модельдерді құру бағытындағы зерттеулердің өзектілігін негіздеу;

– ЖОО АББО-ның киберқауіпсіздік жүйесіндегі инвестициялық процесс параметрлерінің әртүрлі қатынастарын ескере отырып, инвестициялауды басқарудың рационалды стратегияларын табу бойынша шешімдерді қабылдауды қолдау жүйесінің есептеу ядросы үшін модель құру;

– ЖОО АББО-ның киберқорғауын бейімделген басқарудың тұжырымдамалық моделін құру, сондай-ақ қолданушы профилін нақтылау процедураларын автоматтандыруға арналған қолданушының міндеттерін үлестіру моделін құру және ЖОО АББО-ның қолжетімділік құқығын салыстыруға байланысты қолжетімділік құқығын бақылау әдістерін толықтыру;

– ЖОО АББО-ның қорғалуын бағалау міндеттерін шешу үшін көпкритериалды дискретті оңтайландыру әдісін жетілдіру. «ЖОО АББО-ның киберқауіпсіздігін инвестициялауды басқару стратегияларын табу бойынша шешімдерді қабылдауды қолдау жүйесі» компьютерлік бағдарлама құру және модельдің сайлылығын тексеру мақсатында, инвестициялаудың әртүрлі нұсқаларының стратегиялары үшін компьютерлік модельдеуді орындау.

Зерттеу әдістері:

– ЖОО АББО-ның киберқорғауын бейімделген басқарудың концептуалды моделін сипаттау және қолданушылардың қолжетімділік құқықтарын бейімделген басқару міндеттерін шешу үшін - жүйелік талдау әдістері және Петри желілерінің аппараттары қолданылған күрделі жүйелер теориясы әдістері;

– ЖОО АББО-ның киберқауіпсіздігін және ақпараттық ресурстарды техникалық қорғау құралдарын инвестициялаудың рационалды қаржы стратегиясын таңдау бойынша шешімдерді қабылдауды қолдау интеллектуалды жүйесінің есептеу ядросының жаңа модельдерін синтездеуге арналған ойындар теориясының әдістері;

– Эджворт-Парето дискретті оңтайландыру әдісі мен лексикографиялық әдістің комбинациясына негізделген, ЖОО АББО-ның қорғалуын бағалау міндеттерін шешу үшін көпкритериалды дискретті оңтайландыру әдістері;

– диссертацияда ұсынылған шешімдердің тиімділігін бағалау үшін компьютерлік және имитациялық модельдеу әдістері.

Зерттеудің ғылыми жаңалығы:

– ЖОО АББО-ның киберқауіпсіздігін және ақпараттық ресурстарды техникалық қорғау құралдарын инвестициялаудың рационалды қаржы стратегиясын таңдау бойынша шешімдерді қабылдауды қолдау интеллектуалды

жүйесінің есептеу ядросы үшін модельдер ұсынылды. Модельдердің жаңалығы, тәуелді қозғалыстары бар бисызықты көпқадамды сапа ойынының шешімін табуға, ЖОО АББО-ны қорғаушының «қалау» жиынын және рационалды стратегияларын анықтауға мүмкіндік береді;

– ЖОО АББО-дағы киберқауіпті азайту немесе бейтараптандыру үшін қолданушы профилін нақтылау процедураларын автоматтандыруға арналған модель ұсынылды. Модельдің қолданыстағы басқа модельдерден айырмашылығы Петри желілерінің математикалық аппаратына негізделген және күйдің ішкі кеңістігінің қуатын азайтуға мүмкіндік беретін, айнымалыларды ескереді. Атап айқанда, ЖОО АББО-ның төбелеріне қолданушылардың қол жеткізу құқығын регламенттеумен байланысты шешімдерді қабылдауға кететін уақыт шығынын қысқарту есебінен моделдеудің нәтижелігі артады.

– ЖОО АББО-ның төбелеріне қолданушылардың қол жетімділік құқықтарын бақылау әдісі нақтыланды және толықтырылды, қолданыстағы әдістерге қарағанда, толықтыру жаңа немесе қайта қарастырылатын міндеттері үшін қауіпсіздік ережелері мен метрикаларын нақтылау Петри желілерінің шартты белгілерінде сипатталған;

– ЖОО АББО-ның қорғалуын бағалау міндеттерін шешу үшін көпкритериалды дискретті оңтайландыру әдісі жетілдірілді. Қолданыстағы әдістерден айырмашылығы, ұсынып отырған жетілдірілген әдіс Эджворт-Парето дискретті оңтайландыру әдісі мен лексикографиялық әдісті байланыстыруға негізделген, бұл оңтайландырудың екі шарты бар шешімдерді бағалаудың векторлық критерийін құруға мүмкіндік берді: нақты ЖОО АББО үшін ақпараттық ресурстарды техникалық қорғау құралдарының қарастырылып отырған нұсқаларының құндық бағасын және оның техникалық тиімділігін бағалау.

Зерттеудің теориялық маңыздылығы: компьютер қаскүнемдері тарапынан ЖОО АББО жұмысына деструктивті араласу күрделілігінің өсуі жағдайында, ЖОО АББО-ны қорғаудың модельдері мен әдістерінің одан әрі дамуында. Құрылған әдістер мен модельдер тәуелді қозғалыстармен берілген бисызықты көп қадамды сапа ойындары үшін шешімдерді табуға және ЖОО АББО қорғаушысының «қалау» жиынын және рационалды стратегияларын анықтауға мүмкіндік береді. Сонымен қатар, ұсынылған модельдер киберқауіптерді азайту немесе бейтараптандыру үшін ЖОО АББО-да пайдаланушы профильдерін нақтылауға мүмкіндік береді. Бұл пайдаланушылардың ЖОО АББО- ның түйіндерінде қол жеткізу құқықтарының тәртібімен байланысты шешімдер қабылдауға кететін уақытты қысқарту есебінен модельдің нәтижелілігін арттыруға мүмкіндік береді.

Зерттеудің практикалық маңыздылығы: VisualStudio 2017 бағдарламалау ортасында ЖОО АББО-ның қорғалуын бағалау міндеттерін шешу үшін («DSS ШҚҚЖ модулі – ЖОО АББО үшін ақпаратты қорғау жүйесін жобалау кезінде оңтайлы таңдау алгоритмдерін жүзеге асыратын ақпаратты қорғау құралдарын (АҚҚ) таңдау үшін Парето әдісі») және ЖОО АББО-ның

киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау («ЖОО АББО киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)») қолданбалы бағдарламалық өнімдерді құру. «DSS ШҚҚЖ модулі – ақпаратты қорғау құралдарын (АҚҚ) таңдау үшін Парето әдісі», «ЖОО АББО киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» құрылған модельдердің қолданбалы бағдарламалық өнімдері ЖОО АББО-ның қорғау периметрлерін бұзуға әрекет ететін екінші тарап қаншалықты қаржыландыру жасаса да, қаржыландыру процесін сипаттайтын параметрлердің кез-келген қатынасында қорғаушы тарапқа стратегиясының оңтайлы қаржы стратегиясын таңдауға мүмкіндік береді.

Қорғауға ұсынылатын негізгі қағидалар:

– ЖОО АББО ақпаратты қорғау және киберқауіпсіздік жүйелерін инвестициялаудың рационалды қаржы стратегиясын таңдау бойынша шешімдерді қабылдауды қолдау интеллектуалданған жүйелерге арналған модельдер;

– ЖОО АББО киберқатерді азайту немесе бейтараптандыру үшін қолданушы профилін нақтылау процедураларын автоматтандыруға арналған модель;

– ЖОО АББО төбелеріне қолжетімділік құқықтарын бақылау әдісі;

– ЖОО АББО қорғалуын бағалау міндеттерін шешу үшін көпкритериалды дискретті оңтайландырудың жетілдірілген әдісі.

Ізденушінің жеке үлесі: қорғауға ұсынылған диссертациялық жұмыстың барлық негізгі нәтижелері ізденушінің өзі алған нәтижелер, атап айтқанда:

– ЖОО АББО ақпараттық ресурстарын техникалық қорғау құралдары және киберқауіпсіздік жүйелерін инвестициялаудың рационалды қаржы стратегиясын таңдау бойынша шешімдерді қабылдауды қолдау интеллектуалданған жүйелерге арналған модельдер;

– ЖОО АББО киберқатерді азайту немесе бейтараптандыру үшін қолданушы профилін нақтылау процедураларын автоматтандыруға арналған модель;

– ЖОО АББО төбелеріне қолжетімділік құқықтарын бақылау әдісі;

– ЖОО АББО қорғалуын бағалау міндеттерін шешу үшін көпкритериалды дискретті оңтайландырудың жетілдірілген әдісі.

Тақырыптың ғылыми-зерттеу бағдарламаларының жоспарларымен байланысы: Диссертациялық жұмыс халықаралық ғылыми-зерттеу жобасында Абай атындағы ҚазҰПУ мен Экономика Жоғары Мектебі (Мәскеу, Ресей) бірлескен «Жоғары оқу орындарының оқу процесіне цифрлық құралдардың ену мониторингі» тақырыбы аясында жүргізілді (келісім-шарт 19.04.2019 ж. № 19/04).

Зерттеу нәтижелерін сынақтан өткізу: зерттеудің негізгі қағидалары мен нәтижелері халықаралық ғылыми–практикалық конференцияларда: «Part of the Advances in Intelligent Systems and Computing book series» (Warsaw, 2018) «Актуальні питання забеспечення кібербезпеки та захисту інформації» (Киев,

2018), «Проблемы техники и технологий телекоммуникаций» (Уральск, 2018), «Стан та удосконалення безпеки інформаційно - телекоммунікаційних систем» (Украина, 2018), «Проблемы информатики в образовании, управлении, экономике и технике» (Пенза, 2018), «Новые информационные технологии и системы» (Пенза, 2018), «Цілі сталого розвитку третього тисячоліття: виклики для університетів наук про життя» (Київ, 2018), «International Journal of Civil Engineering and Technology» (India,2019), «Актуальные вопросы экономического и социального развития в условиях цифровизации» (Семей, 2019), «Университет–ой-пікірлер аймағы» (Ақтау, 2019), «Математикалық модельдеу мен ақпараттық технологиялар білімде және ғылымда» (Алматы, 2020), сонымен қатар Абай атындағы Қазақ ұлттық педагогикалық университеті Информатика және білімді ақпараттандыру кафедрасының «Білімді ақпараттандыру және оқыту мәселелері» атты ғылыми – әдістемелік семинарда талқыланды.

Диссертацияның нәтижелері Украинаның БТПҰУ, ақпараттық технологиялар факультетінің оқу процесіне (енгізу актісі 12.03.2020 № 16-35) және «Семей қаласының Шәкәрім атындағы университет» коммерциялық емес акционерлік қоғам, «Ақпараттық-коммуникациялық технологиялар» факультетінің оқу процесіне енгізілді (енгізу актісі 10.08.2020 № 255), Қазақстанның ЖШС «Kaspersky LAB KZ» лабораториясында сынақтан өтті (енгізу актісі 10.02.2020).

Құрылған бағдарламалық өнімдерді қолдану, ЖОО АББО-ның киберқауіпсіздік контурларын құруға кеткен шығындарды, бастапқы жоспарланған параметрлермен салыстырғанда шамамен 11-14% - ға қысқартуға мүмкіндік берді.

Ұсынылған әдістер, модельдер және құрылған бағдарламалық өнімдер Қазақстанның басқа да ЖОО АББО-ның киберқорғау дәрежесін арттыру үшін пайдаланылуы мүмкін.

Зерттеу нәтижелері бойынша жарияланымдар: диссертация тақырыбы бойынша 21 жұмыс жарияланған, оның 5 - ҚР Білім және Ғылым министрлігі Білім және ғылым саласында сапаны қамтамасыз ету комитеті ұсынған басылымдарда, 3 мақала Scopus мәліметтер қорына кіретін басылымдарда, 11 мақала халықаралық ғылыми-тәжірибелік конференция жинақтарында (оның ішінде, шетелдік конференциялардың материалдар жинақтарында – 7), жақын шетелдің ғылыми журналдарында - 2 мақала жарияланған.

Диссертацияның құрылымы: диссертация кіріспеден, төрт тараудан, қорытындыдан, пайдаланылған әдебиеттердің тізімінен және қосымшалардан тұрады.

Кіріспеде зерттеудің ғылыми аппараты ұсынылған, зерттеу тақырыбының өзектілігі, оның теория мен практикада құрылу деңгейі ашылған, зерттеу проблемасының негізінде жатқан қарама-қайшылық қалыптасқан, зерттеудің нысаны, мақсаты, болжамы, міндеттері анықталған, ғылыми жаңалығы, зерттеудің теориялық және практикалық маңыздылығы ашылған, зерттеудің

кезеңдері мен әдістері анықталған, қорғауға шығарылған модельдер мен әдістер атап көрсетілген.

Бірінші тарауда жоғары оқу орындарының ақпараттық білім беру ортасын қорғауды қамтамасыз ету сферасында жасалған зерттеулерге шолу және талдау жасалды. Әлемде көптеген өнеркәсіптері дамыған мемлекеттерде білім берудің цифрлық жүйелерін дамытудың артықшылығы, тек педагогикалық қызмет саласындағы мамандарға ғана емес, сонымен қатар ақпараттық-коммуникациялық технологиялар (АКТ) мамандарына да тиісті техникалық-әдістемелік қолдауды талап ететіні көрсетілген. Көптеген елдерде ақпараттық ресурстарға қолжетімділікті жаһандандырудың қалыптасқан түрі заманауи жоғары оқу орындарының қызметтерінің барлық салаларына ақпараттық-коммуникациялық технологияларды енгізу міндеттерін өзекті етеді деп негізделген. ЖОО АББО-ның киберқауіпсіздік жүйесіндегі инвестициялық процесс параметрлерінің әртүрлі қатынастарын ескере отырып инвестициялауды басқару стратегияларын табу бойынша шешімдерді қабылдауды қолдау жүйесі үшін модель құру бағытындағы зерттеулердің өзектілігі негізделген. ЖОО киберқауіпсіздік стратегияларының ішінен, инвестициялауды басқару стратегияларын табу бойынша міндеттерді шешуге компьютерлік қолдау қажеттілігі көрсетілген.

Екінші тарауда ЖОО АББО-ның ақпаратты қорғау және киберқауіпсіздік жүйелерін инвестициялаудың рационалды қаржы стратегиясын таңдау бойынша шешімдерді қабылдауды қолдау интеллектуалды жүйесінің, есептеу ядросы үшін жаңа модельдер құрылған. Бірінші модель жоғары оқу орындарының ақпараттық білім беру ортасының киберқорғау құралдарын қаржыландырудың рационалды стратегияларын таңдау үшін арналған. Бұл модельдің шешімі ақпараты толық берілмеген жағдай үшін, көпқадамды сапа ойындар теориясының әдістерінің көмегімен табылады. Екінші модель жоғары оқу орындарының ақпараттық білім беру ортасын қорғаушының «қалау» жиынын және рационалды стратегияларын анықтау үшін қолданылады. Екінші модельде ойыншылардың кезектесіп жүретін бірнеше терминалды беттері бар, бисызықты көп қадамды сапа ойыны нұсқасы қарастырылады.

Тарауда ұсынылған модельдер, қолданыстағы шешімдерге қарағанда, ЖОО АББО-ны қорғаушы тарапына ақпараттық жүйелерді қорғау кезінде ресурсттардың шығындарын талап ететін жағдайлардың нұсқалары үшін шешімдерді неғұрлым тиімді табуға мүмкіндік берді. Тарауда есептеу эксперименттерінің нәтижелері сипатталған. ЖОО АББО-ның қорғаушысы және киберқауіпсіздік шекарасын өтуге ұмтылатын компьютер қаскүнемдері жағынан, ойын параметрлерінің барлық жағдайлары үшін шешімдер қарастырылған. ЖОО АББО қорғаушысының оңтайлы әрекеттерінің (қаржы стратегияларының) нұсқалары табылған. ЖОО АББО-ны қорғаушы тарапына хакердің қаржы ресурстарының жағдайы бойынша мәліметтер толық берілмеген жағдайлар қарастырылды. Есептеу және шынайы эксперименттер жүргізу барысында, ұсынылған математикалық модельдердің сайлылығы

расталды. Есептеу эксперименттері нәтижелерінің практикалық мәліметтерден (қолданыстағы мәліметтерден) ауытқуы 12% - дан аспайды.

Үшінші тарауда ЖОО АББО киберқорғауын бейімделген басқарудың тұжырымдамалық моделі сипатталған. Петри желілерінің аппаратын пайдалана отырып, ЖОО жергілікті есептеу желілері (ЖЕЖ) қолданушыларының қолжетімділік құқықтарын бейімделген басқару есебін шешудің мысалы қарастырған. Сәйкес келетін модель жүзеге асырылды және PIPE v4.3.0 және Petri.NetSimulator. 2.017 пакеттерде имитациялық модельдеу орындалды. Сонымен қатар, тарауда ЖОО АББО-дағы киберқатерді азайту немесе бейтараптандыру үшін, ЖЕЖ қолданушы профилін нақтылау процедураларын автоматтандыру мүмкіндіктері көрсетілген. Пайдаланушылар тағайындаған жергілікті есептеу желілерінде міндеттерді үлестіру моделі сипатталған. Петри желілерінің математикалық аппараты модель үшін база болды. Қолжетімділік құқықтарын бақылау әдісі (ҚҚБӘ) нақтыланды және толықтырылды. Нақтылаулар қауіпсіздік саясатының міндеттері және талаптары бойынша сұрлатын қолжетімділік құқықтарын салыстыру аспектілеріне қатысты. Сонымен қатар, ЖОО АББО міндеттері мен қолжетімділікке рұқсат етілген төбелердің арасындағы сәйкестігі ескерілді. ЖОО АББО төбелері үшін де тиісті құқықтары бар абоненттердің қолжетімділік құқығын салыстыру процедурасы қарастырылған. Модель нақты ЖОО АББО үшін қауіпсіздік саясатының ағымдағы көрсеткіштерін және соңғы нақтылаулар енгізілген қауіпсіздік метрикасын ескереді. Жаңа міндеттер немесе қайта қарастырылатын міндеттер үшін қауіпсіздік ережелері мен метрикаларын нақтылау, Петри желілерінің шартты белгілері арқылы сипатталған.

Төртінші тарауда ЖОО АББО қорғалуын бағалау міндеттерін шешу үшін көпкритериалды дискретті оңтайландырудың әдісі жетілдірілді. Шешім Эджворт-Парето дискретті оңтайландыру әдісі мен лексикографикалық әдістің комбинациясына негізделген. Құрамында оңтайлылықтың екі шарты бар, шешімді бағалаудың векторлық критерийі жасалды: нақты ЖОО АББО ақпаратты қорғау құралдарының (АҚҚ) қарастырылып отырған нұсқаларының құндық бағасын және оның техникалық тиімділігінің бағасын бағалау. Сонымен қатар, тарауда ЖОО АББО ақпараттық қауіпсіздік және киберқауіпсіздік жүйелерін жүзеге асырудың, барлық ықтимал нұсқаларын ескере отырып, ЖОО АББО үшін АҚҚ оңтайлы таңдау алгоритмды құру және сынақ нәтижелері сипатталған.Жоғары оқу орнының АББО үшін АҚЖ жобалау кезінде оңтайлы таңдау алгоритмдерін жүзеге асыратын «DSS ШҚҚЖ модулі АҚЖ таңдау үшін Парето әдісі» компьютерлік бағдарламасы құрылған және сыналған. «ЖОО АББО киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» құрылған бағдарламалық өнім ЖОО АББО қорғаушысына киберқауіпсіздік құралдарын қаржыландырудың оңтайлы стратегиясын табуға мүмкіндік беретін, бисызықты дифференциалдық ойындардың жаңа класын қолдануға негізделген. Құрылған «DSS» бағдарламалық өнімі, ЖОО АББО ақпаратты қорғау және КҚ құралдарын

инвестициялауға жұмсалатын нақты мәліметтермен болжанған мәліметтердің айырмашылығын азайтуға мүмкіндік береді.

Қорытындыда диссертациялық зерттеудің теориялық және практикалық нәтижелері жинақталған, қорғауға шығарылатын модельдер мен әдістер шынайылығын растайтын негізгі қорытындылар тұжырымдалған.

1 ЖОҒАРЫ ОҚУ ОРЫНДАРЫНЫҢ АҚПАРАТТЫҚ БІЛІМ БЕРУ ОРТАСЫН (ЖОО АББО) ҚОРҒАУДЫ ҚАМТАМАСЫЗ ЕТУ САЛАСЫНДАҒЫ АЛДЫҢҒЫ ЗЕРТТЕУЛЕРГЕ ШОЛУ ЖӘНЕ ТАЛДАУ

1.1 Жоғары оқу орынының ақпараттық білім беру ортасы

Әлемнің көптеген өнеркәсіптері дамыған мемлекеттерде білім берудің цифрлық жүйелерін дамытудың артықшылығы, тек педагогикалық қызмет саласындағы мамандарға ғана емес, сонымен қатар ақпараттық-коммуникациялық технологиялар (АКТ) мамандарына да тиісті техникалық-әдістемелік қолдауды талап етті. Осылайша, көптеген елдерде ақпараттық ресурстарға қолжетімділікті жаһандандырудың қалыптасқан түрі заманауи жоғары оқу орындарының қызметтерінің барлық салаларына ақпараттық-коммуникациялық технологияларды енгізу міндеттерін өзекті етеді [13].

Өткен ғасырдың 90-жылдарында отандық және шетелдік әдебиеттерде білім беруді ақпараттандырудың жаңа мүмкіндіктері туралы түсініктер айтылған. Атап айтқанда, бірқатар зерттеушілер, олардын ішінде В.В. Яворский [14], А.В.Хуторской [15], Л.Н.Кечиев [16], Г.П.Путилов [16] и С.Р.Тумковский [16], Г.В. Абрамян [17], И.Г. Захарова [18], Б.С. Ахметов [20], Е.Ы Бидайбеков [19], Я.А.Ваграменко [21] ақпараттық технологиялар бірқатар зерттеулерде «ақпараттық білім беру кеңістігі» және «ақпараттық білім беру ортасы» деп аталған, жаңа дамып келе жатқан орта мен білім беру кеңістігін жобалау мен модельдеуге негіз болатыны туралы айтқан.

Ақпараттық білім беру ортасы (АББО) ұғымы, онымен тығыз байланысты ақпараттық білім беру кеңістігі ұғымы сияқты, бірнеше анықтамалармен берілгеніне қарамастан, жеткілікті түрде бірмағыналы және қайшылықсыз сипатталады. Мысалы, Л.Н.Кечиева, Г.П.Путилова және С.Р.Тумковскийдің пікірі бойынша, ақпараттық білім беру ортасы оқыту қызметін жүзеге асыру үшін пайдаланылатын компьютерлік құралдар мен олардың жұмыс істеу тәсілдерінің жиынтығы [16].

Сонымен қатар, басқа да ғылыми жұмыстардан, біртұтас АББО деп, білім алушыларды, мұғалімдерді, ата-аналарды, оқу мекемелерінің әкімшілігін және қоғамды біртұтас технологиялық құралдармен ақпараттық қамтамасыз ететін компьютерлік техниканы қолдануға негізделген бағдарламалық-телекоммуникациялық орта деп түсінуге болады. Соңғы анықтамаға сәйкес, мұндай орта оқу процесі мен оқу мекемесін басқаруға ақпараттық қолдау көрсетуге, оқу процесінің барлық қатысушыларын оның барысы мен нәтижелері туралы, сонымен қатар оқудан тыс іс-шаралар туралы ақпараттандыруға бағытталған. Осы зерттеу жұмысында жоғары оқу орынының (ЖОО) ақпараттық ресурстары ретінде жоғары оқу орынының студенттері, магистранттары, докторантары, оқытушылары, әкімшілігі және қызметкерлері тұтынушы ретінде пайдаланатын немесе өздері беретін кез-келген мәліметтер, ақпараттар, мағлұматтар қарастырылады [19].

АББО-ны жобалау мен құрудың техникалық аспектілерін зерттеген Г.П.Путиловтың басылымдарында, «... АББО-ны қолданатын салалар тек

жоғары оқу орынымен шектелмейді»- деп, айтылған. Ірі өнеркәсіп мекемелері, әскери және азаматтық мекемелер кадрларды даярлауды және қайта даярлауды өздері жүзеге асырады. Сонымен қатар, өнеркәсіптері дамыған елдерде жаңа күрделі машиналар мен технологияларды меңгеру және өнеркәсіпке енгізу процесін жеңілдететін және тездететін, компьютерлік оқыту жүйелерімен жабдықтау стандарт жағдай. Шетелдерде АББО-ны құруды, оның ғылыми күрделілігінің жоғары болуына және жобалаушылар, психологтар, пән оқытушылары, компьютерлік дизайнерлер сияқты әртүрлі мамандықтағы жоғары білікті мамандармен бірлесіп жұмыс істеу қажеттілігіне байланысты өте қымбат тұратын жұмыс деп санайды. Осыған қарамастан, көптеген ірі шетелдік фирмалар оқу орындарында АББО-ны құру жобаларын қаржыландырады және осы салада өздерінің зерттеулерін жүргізеді [16, с.41].

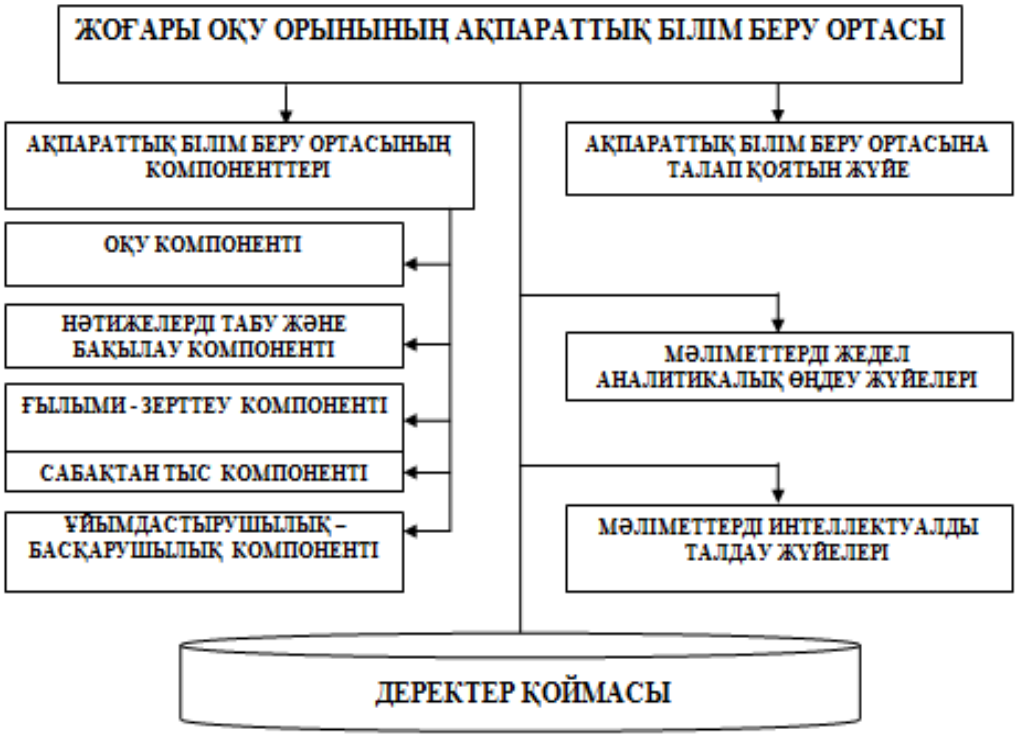
Егер берілген анықтамалар мен түсініктерден АББО-ның мәні туралы ең болмағанда жуық түсінік алуға болатын болса, онда АББО-ның рационалды компонентерінің құрылымын, мүмкіндіктерінің тізімін, тиімді пайдалану аймақтарын, АББО-ны құру және жұмыс істеу ерекшеліктерін анықтау үшін педагогикалық және технологиялық салаларда егжей-тегжейлі зерттеулер қажет.

Білім беруді ақпараттандыру саласындағы кейбір зерттеулер, атап айтқанда, ақпараттық ортада оқытушының кәсіби қалыптасу аспектісін Г.В. Абрамян жүзеге асырды. Бірақ, оның диссертациясында заманауи педагогтың қызметін тиімді жоғарлататын қазіргі заманғы ақпараттық технологиялардың дамуына және практикада қолдануына тура және жанама байланысты негізделген факторлар анықталғанына қарамастан, бұл жұмыста жоғары оқу орнының АББО-ны құрудың мүмкін жолдарын, осындай ортаның мүмкін компоненттік құрамын, оны құру мен пайдаланудың мүмкін теориялық тәсілдері туралы міндет қозғамайды [17].

И. Г.Захарованың диссертациялық жұмысы ақпараттық білім беру ортасы ұғымын зерттеу тақырыбына арналған [18]. Бірақ оның жұмысында ортаның неғұрлым тиімді компоненттерден тұратын құрамының егжей-тегжейлі сипаттамасы мен негіздемесі жоқ, ортаға енгізуге ұсынылатын ақпараттық және телекоммуникациялық технологиялардың негізгі түрлері анықталған жоқ, орта моделін алдын ала анықтаумен байланысты теориялық тәсіл ұсынылмайды, шашыраңқы ақпараттық ресурстарды біріктіру және біріздендіру жолдары қарастырылмаған.

Б.С.Ахметов, Е.Ы.Бидайбеков, В.В.Яворский еңбектерінде заманауи жоғары оқу орынының қызметтерінің барлық салаларын ақпараттандыру процестерімен байланысты барлық факторларды жинауға және жүйелеуге негізделген интеграциялау және жүйелеу жұмыстары жүргізілді. Зерттеу барысында алынған жоғары білім беру жүйесі мекемелерінің оқу, бақылау-өлшеу, сабақтан тыс, ғылыми-зерттеу және ұйымдастырушылық-басқару қызметін ақпараттандырудың ерекшелігі мен тиімділігіне әсер ететін барлық бірыңғай талаптарды, компоненттерді, ақпараттық ресурстар мен

технологияларды жүйелі түрде біріктіру нәтижесінде көрсетілген ЖОО АББО-ның көп компонентті моделі [19,20,21] құрылды (сурет 1).



Сурет 1 – Жоғыры оқу орынының АББО-ның көпкомпонентті моделінің жалпы құрылымы

Осы құрылымның әрбір элементі жоғарыда аталған ортаның бес компонентінің құрылымы мен мазмұнын, жалпы ақпараттық білім беру ортасын құруға және пайдалануға қойылатын жалпы талаптарды, ақпараттық білім беру ортасымен жұмыс істеуге кадрларды даярлауға қойылатын талаптарды, ЖОО-да ақпараттық білім беру ортасын пайдаланудың негізгі артықшылықтары мен перспективаларын сипаттайтын графтар жүйесінің көмегімен нақтыланады [21].

Модельдің мұндай құрылымы мен мазмұны және мүмкін болатын ақпараттық ресурстарды аса маңызды талаптармен интеграциялау, құрылған көпкомпонентті модельді максималды педагогикалық әсері бар ЖОО АББО-ны құруға және қолдануға теориялық – әдістемелік нұсқалық ретінде қарастыруға мүмкіндік береді.

Алайда, ЖОО АББО-ны дамыту міндеттеріне арналған осы және басқа көптеген зерттеу жұмыстарында ЖОО АББО-ға компьютер қаскүнемдері тарапынан болатын деструктивті араласуының кез-келген түрінен ақпараттарды қорғауға және киберқауіпсіздікті қамтамасыз етуге байланысты қарастырылмаған аспектілер бар. Сонымен, жоғары оқу орнының ақпараттық білім беру ортасы дегеніміз – жоғары оқу орнының аппараттық, бағдарламалық, ақпараттық ресурстарының және кіріктірілген ақпараттық компьютерлік

желілердің жиынтығы және кез-келген маңызды компьютерлік жүйе сияқты кибершабуылға ұшырауы мүмкін жүйе. Мысалы, ZOOM жүйесі, BilimLand, Daryn.Online, Opiq оқу платформалары және тағы басқа.

1.2 Заманауи жоғары оқу орнының қауіпсіз ақпараттық білім беру ортасын қалыптастырудың алғышарттары

Білім берудің жаһандануы ЖОО-да ақпараттық технологиялар мен жүйелерді қолдану міндеттерін бірінші орынға қойды. Бірақ, қызметкерлердің, студенттердің ақпараттық қауіпсіздігін (АҚ) және киберқауіпсіздігін (КҚ) қамтамасыз ету міндеттеріне жеткілікті түрде көңіл бөлінбеген.

Заманауи оқу орындары өздерінің қабырғаларында жоғары білікті оқытушыларды, ғылыми бөлімдердің қызметкерлерін, студенттерді, сонымен қатар қызмет көрсететін персоналдарды біріктіреді.

Алайда, оқу-әдістемелік сипаттағы әртүрлі ақпараттарды, мысалы, ЖОО–дағы процестерге қатысты мәліметтерді, қызметкерлер мен студенттердің жеке мәліметтерін үнемі жинақтай отырып, ЖОО АТ-ның мамандары қосымша проблемаларға тап болды. Ең алдымен, шашыраңқы және әр түрлі форматтағы ақпараттық ресурстарды жинақтау және практикада қолдану кезінде нақты процедураның жоқтығын атап айтуға болады. Көбіне, бұл ресурстар АҚ-ны және КҚ–ны тексерген кезде жиі өтпей қалады. ЖОО АББО – да орнатылған көптеген бағдарламалық өнімдер бір-бірімен байланысты емес, себебі олар әр түрлі бағдарламалық жабдықтардан, олардың ішінде тіпті күмәнді дерек көздерден алынған, сондықтан ЖОО АББО-ға потенциалды қауіп төндіруі мүмкін [20].

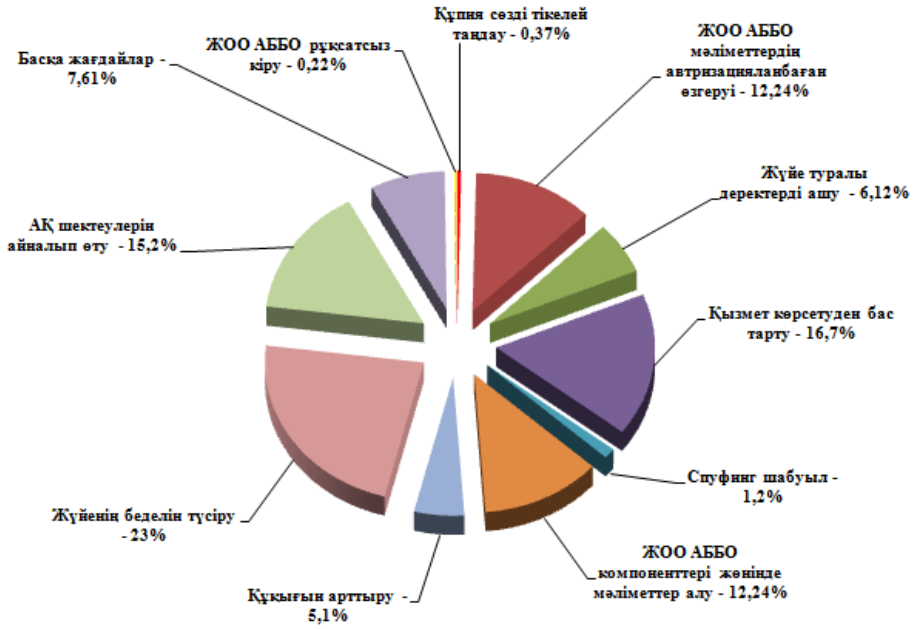
ЖОО ақпараттық-коммуникациялық жүйелерінде (АКЖ) сақталатын және қолданылатын және қорғалу керек ақпаратқа мыналарды жатқызуға болады [14]:студенттердің, оқытушылардың, ғылыми қызметкерлердің, қызмет көрсетуші персоналдардың жеке мәліметтері; оқу орнының интеллектуалды меншігі болып саналатын цифрланған ақпарат; оқу процесін қамтамасыз ететін ақпараттық массивтер (мысалы, мультимедиялық контенттер, мәліметтер базасы, оқыту бағдарламалары). Ал осы жүйе қауіпсіздігі әрбір ЖОО оқытушысына таныс мәселе.

Бұл ақпарат студенттердің және қызметкерлердің тарапынан болатын бұзақылық ниетпен немесе сырқы (ішкі) компьютер қаскүнемдері тарапынан ұрлау немесе бұрмалау нысаны ретінде әрекет етуі мүмкін.

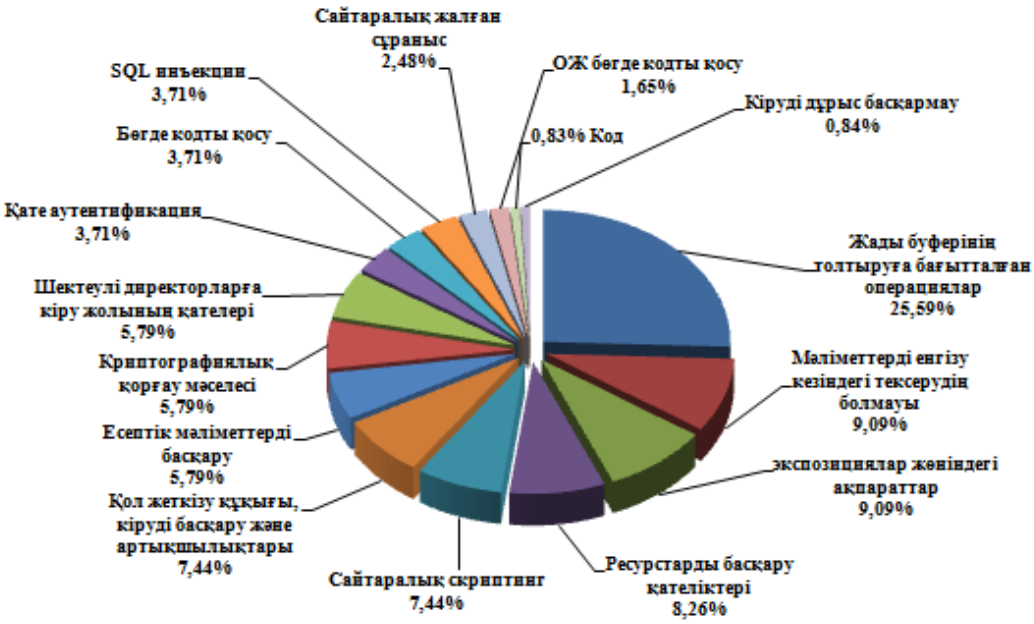
Диссертацилық зерттеу барысында мемлекеттік ұйымдар үшін, атап айтқанда, ірі жоғары оқу орындары үшін өзекті міндеттерімен айналысатын халықаралық компаниялардың АҚ және КҚ бойынша жүргізген аудитінің нәтижелері бойынша талдау жүргізілді. Бірінші кезекте Еуропалық Одаққа кіретін мемлекеттер, АҚШ және Канада мемлекеттері туралы айтып отырмыз [23].Осыған ұқсас зерттеулердің нәтижелері көрсеткендей [24, с.48], сондай-ақ [25-27] зерттеу жұмыстарында келтірілген мәліметтер көрсеткендей, буфердің толып кетуіне және криптографиялық хаттамалардың бұзылуына бағытталған нақты мақсатты шабуылдарды есепке алмағанда құқық бұзушылықтардың

едәуір бөлігі ЖОО АББО –да мәліметтердің рұқсатсыз өзгеруімен (>12 %), ЖОО АББО –дағы АҚ- ның шектеулер саясатын айналып өту (>15 %), аутентификация процедурасының жеткіліксіз қорғалуымен және т.б. байланысты (суреттер 2,3).

Зерттеулердегі [28,29] мәліметтерге сүйенсек ЖОО АББО-ға жасалатын кибершабуылдардың мақсаттары, нысандары мен субъектілері әртүрлі болуы мүмкін (кесте 1).



Сурет 2- ЖОО АББО-дағы осалдықтардың таралуы



Сурет 3 - ЖОО АББО-ға жасалатын шабуылдар

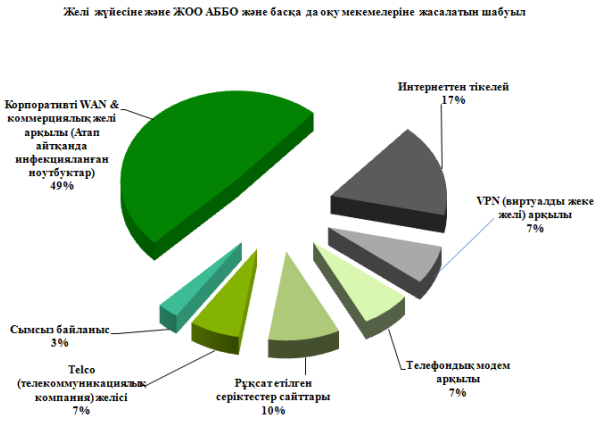
Зерттеулерде [23,34] ЖОО АКЖ-сы үшін болатын вирустық бағдарламалық жабдықтардың қарқынды даму эволюциясымен байланысты қауіптерлер туралы айтылған, олар ЖОО АББО-ның көптеген компоненттеріне үлкен қауіп төндіреді. Заманауи вирустар тек Windows-тың ОЖ –сына ғана емес, сонымен қатар ЖОО АББО –ның құрылымындағы басқа да жүйелер үшін болуы мүмкін, мысалы, HDI және сенсорлық ішкі жүйелер үшін қауіпті (сурет 4).

Кесте 1-ЖОО АББО-ға жасалатын кибершабуылдың мақсаттары, нысандары және субъектілері

Кибершабуылдың түрлері			
Кибершпионаж-мәліметтердің жасырын (жарияланбаған) байланыс арналарын, АЖ бағдарламаларын және басқа да мүмкіндіктерді пайдалана отырып, рұқсатсыз тарату	Кибераудит-хакерлік және «достық» кибершабуылдардың сценарийлерін құру, ЖОО АББО-дағы осалдықтарды іздеу.	Кибер-алаяқтық-студенттік билеттерді қолдан жасау, журналдағы бағаларды өзгерту және оқу материалдарын өзгерту және т.б.	Киберсаботаж- ЖОО АББО ресурстарының есебінен өнімділіктің төмендеуі,атап айтқанда, оқу процесі толығымен тоқтатылғанға дейін.
Кибершабуыл нысандары			
ЖОО-ның ақпараттық жүйелері (АЖ)	ЖОО-ның жеке меншік немесе арнайы тапсырыспен жасалған программалық жабдықтары	ЖОО-ның мәліметтер қоры	Жергілікті желі компоненттері
ЖОО АББО-ға жасалатын кибершабуыл нысандары: ЖОО АЖ, қашықтан оқыту жүйесі, мәліметтер базасының серверлері, студенттердің, оқытушылардың, ғылыми қызметкерлердің, қызмет көрсетуші персоналдардың жеке мәліметтері және т.б.			
Шабуылдаушы тарап			
Тәжірибесіз хакерлер, кәсіби хакерлер, бәсекелестер, инсайдерлер, ұйымдасқан қылмыстық топтар және т. б. Сонымен қатар, шабуылдаушы тараптың техникалық жабдықталу және құзыреттілігінің деңгейі жеткілікті түрде жоғары болуы мүмкін.			

Сурет 4 - ЖОО АББО-ға жасалатын
вирустық шабуылдар (ену әдістері)

Жоғары оқу орындарының қазіргі заманғы есептеу желілері, әдетте, корпоративтік ақпараттық жүйелермен (КАЖ) байланысты, жалпы пайдаланымдағы желілерге кіруге шектеу қойылмайды. Бұл оқу процесін жүзеге асырудың тиімділігін арттырады, бірақ ЖОО АББО үшін, ЖОО-ның компьютерленген басқару жүйелері үшін (мысалы, қызметкерлер мен студенттерді есепке алу жүйелері, материалдық құндылықтарды есепке алу және т.б.) қосымша осалдықтар тудырады. Сонымен қатар, мұндай кибершабуылдар ЖОО АББО-ның студенттік және оқытушылар кампустарының жергілікті желілерімен, сондай-ақ жаһандық желілермен түйіндесу элементтері (коммутатор) арқылы жүзеге асырылады (сурет 5).

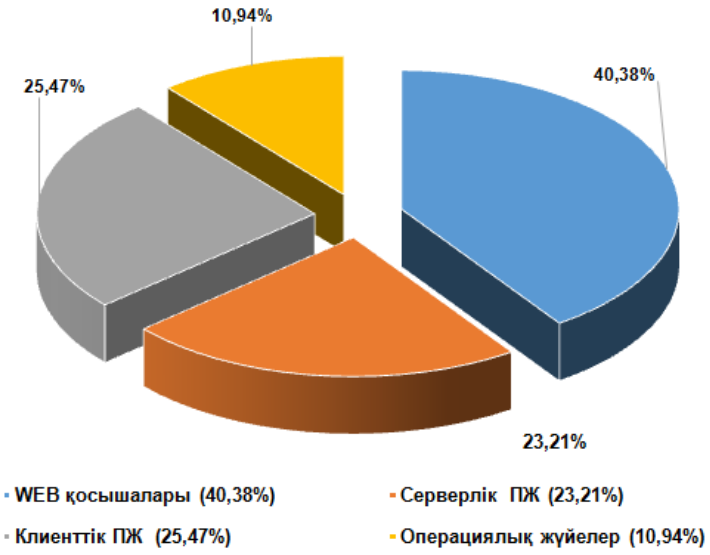


Сурет 5- ЖОО АББО –ға және ЖОО-ның бақару жүйесіне жасалатын
шабуылдардың даму көздері мен арналары

АҚ-ның және КҚ-ның проблемаларымен айналысатын әртүрлі компаниялардың, оның ішінде мемлекеттік мекемелер үшін (ЕО мен АҚШ-тың ірі жоғары оқу орындарын қоса алғанда) талдаушылары кибероқиғалардың көпжылдық статистикасы негізінде АКЖ-дағы осалдықтардың таралуы

бойынша мынадай деректерді келтіреді: Web қосымшалардың үлесіне осалдықтардың >40%, серверлік бағдарламалық жабдықтарға (БЖ) шамамен 23 %, клиенттік БЖ-ға >25% және операциялық жүйелерге шамамен 11% тиесілі (сурет 6) [7].

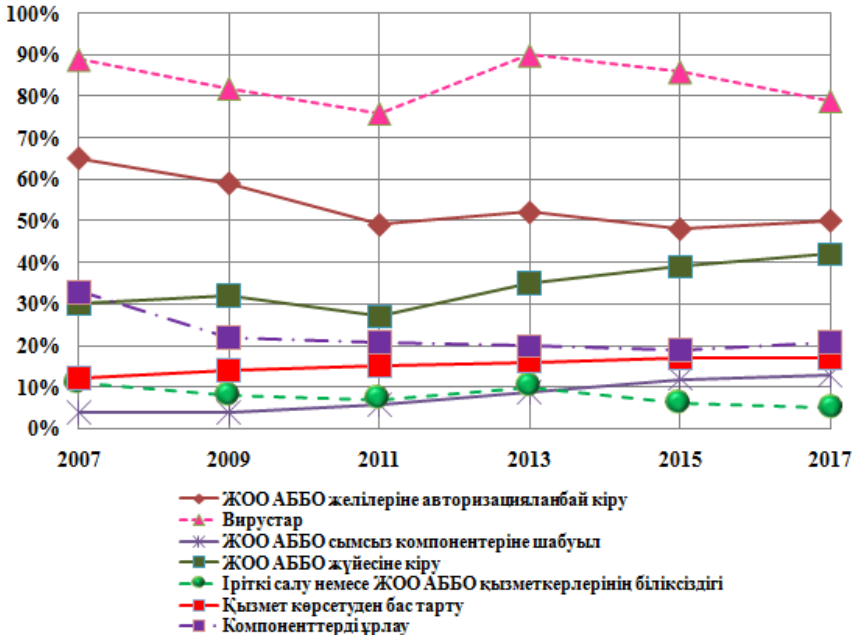
Басқа зерттеу жұмыстарында да осыған ұқсас мәліметтер келтіріледі. Зерттеу жұмыстарындағы [26] мәліметтер бойынша, 2010–2018 жылдары анықталған осалдықтардың мөлшері 40% ЖОО АББО Web-қосымшасына тиісті екені көрсетілген.



Сурет 6 - ЖОО АББО қосымшаларының түрлері бойынша осалдықтардың таралуы (2010-2018 ж. аралығында)

АҚ және КҚ саласындағы сарапшылар бірнеше жыл қатарынан ЖОО АББО - дағы кибероқиғалар және кибершабуылдар санының тұрақты өсуін көрсететін тенденцияны тіркеді (сурет 7). Бұл жағдайды жалпы пайдаланымдағы желілерге қосылған ЖОО-ның жергілікті желілері санының өсуімен түсіндіруге болады [23-25]. ЖОО АББО-ның қорғалуын бағалау проблемасына арналған басылымдарда [24, с.36] ЖОО АКЖ-да айналымда болатын ақпаратты қорғау жөніндегі техникалық міндеттерден басқа, ЖОО АҚ-ны және КҚ-ны қамтамасыз етуге бағытталған ақпараттық тәуекелдерді кезең-кезеңімен талдау және енгізілген іс-шаралардың тиімділігін бақылау қажет екені көрсетілген. Осы процедуралар төмендегі жағдайларды ескеруге мүмкіндік береді: ақпаратты қорғау міндеттерінде талаптардың өзгеріп тұруы(мысалы, контентті қорғаудан бастап студенттердің және қызметкерлердің жеке ақпараттарын қорғауға дейін); ЖОО АКЖ – да жаңа киберқатерлердің және осалдықтардың пайда болу мүмкіндігінің ықтималдылығы; уақыт өте келе ақпаратты қорғау бойынша жүзеге асырылған шаралардың тиімділігінің төмендеуі; жабдықтар мен бағдарламалық қамтамасыз ету физикалық ескіргендіктен ЖОО АББО - да ақпаратты өңдеу процесінің сенімділігінің төмендеуі. Жоғары оқу орындарында және басқа да оқу орындарында сымсыз, оның ішінде сенсорлық желілер мен технологияларды белсенді енгізу және

кеңінен пайдалану [25], қызмет көрсетуден бас тарту - кибершабуылдар класы үшін жаңа осалдықтар тудырды.



Сурет 7- ЖОО АББО үшін киберқатер динамикасы

Сонымен қатар, [26, p.633] зерттеулерде көрсетілгендей, рұқсат етілмеген қолжетімділіктен (РЕҚ) ең аз қорғалған көбінесе сенсорлық төбелер болып саналады. Сонымен қатар, олардың ресурстары мен қызмет ету мерзімі энергиямен жабдықталуына, қосу-өшіру циклдерінің санына байланысты, бұл хакерлер үшін нысана болуы мүмкін. Осылайша, шабуылдаушы ЖОО АББО-ның сенсорлық төбесіне толық бақылау жасау үшін осындай шектеулерді қолдана алады, мысалы, ЖОО қабырғасында оқу үшін немесе көрсетілетін басқа да қызметтер үшін төлем жасауды жүзеге асыратын терминалдың үстінен бақылау жасау (жатақхана, интернет қызметі, спорт залы немесе т. б. үшін төлем жасау). Сенсорлық төбелердің беделін оңай түсіруге болады, атап айтқанда, DoS-шабуылдарға жүгіну арқылы. ЖОО АББО-ның дамуына және жаңаруына қарай оған бөгде провайдерлердің модульдері мен компоненттері енгізіледі, атап айтқанда, мұндай компоненттер ЖОО АББО АҚ үшін жауап бере алады. Бірақ, мұндай жаңару кезінде олардың киберқауіпсіздігін алдын-ала тестілеу процедурасын жүргізу қажет, себебі мұндай компоненттер потенциалды шабуылдардың алдында осал болуы мүмкін. Сондай-ақ, [26-28] зерттеулерлерде, мемлекеттік құрылымдардың АКЖ- ға бағытталып жүргізілген нәтижелі кибершабуылдардың күрделілігін төмендету міндеті қарастырылған. Атап айтқанда, нәтижелі шабуылдардың күрделілік деңгейі ең жоғарғы мән - 2004 жылы 87 % -дан , 2018 жылы 46 % -ға төмендеді (сурет 8). Алайда, осы уақыт аралығында АКЖ-да орташа күрделіліктегі осалдықтар саны 5% - дан 44% - ға дейін өсті. АКЖ-ғы күрделі осалдықтарға жасалған шабуылдар соңғы онжылдықта шамамен бірдей деңгейде қалды және 3- 4% - дан аспайды [25, с.169]. Өткен нәтижелермен салыстырғанда мұндай талдауды

егжей-тегжейлі жүргізу, сайып келгенде, ЖОО АББО-ның АҚ және КҚ үшін рұқсат етілген тәуекел деңгейлерін анықтайды [27, p.643].

Жоғарыда аталған міндеттерді шешудің тәсілдері көптеген зерттеулерде [23-29] сипатталған, бұл тәсілдер коммерциялық кәсіпорындар мен мекемелер үшін туындаған міндеттерді шешуге мүмкіндік берді. Алайда, ЖОО-да ақпараттық ресурстарға қолжетімділікті ұйымдастыру ерекшелігі өзгеше болғандықтан, АҚ-ны және КҚ-ны техникалық – ұйымдастыруды басқаруда да ерекшелік болады. Көптеген жоғары оқу орындарында (мектептерде, колледждерде, ЖОО-да, студенттік кампустарда, кітапханаларда және т.б.) ақпаратты қорғау құралдары мен жүйелерін және киберқауіпсіздікті қаржыландыру міндеттерін шешудің дәстүрлі тәсілі сақталуда [29, с.85]. КҚ жүйелерін қаржыландыру стратегиясының басым бөлігі антивирустық бағдарламаларға және және салыстырмалы түрде күрделі емес желілік қорғау құралдарына қаражат бөлуді ғана болжайды [26, p.649]. Бұл ЖОО-ның киберқорғау бойынша қарапайым қаржы стратегиялары. Тіпті ақпараттық және кибернетикалық қауіпсіздік қызметінің тәжірибелі администраторлары да ЖОО- ның компьютерлік жүйелері мен желілеріне кибершабуылдар кезінде оқиғалардың дамуының ең нашар нұсқасына әрдайым дайын бола бермейді [28]. Ақпаратты қорғау тарабына КҚ-ның құралдарын қаржыландыру жөніндегі дәстүрлі тәсілдерді өзгертуге өз назарын аударуы қажет. Мысалы, ЖОО-ның компьютерлік жүйелері мен желілерін потенциалды бұзуды анықтауды және бұғаттауды қамтитын саясатқа ауыса отырып, КҚ-ны инвестициялау стратегиясының қаржы компоненттерін таңдау [26, p.645].

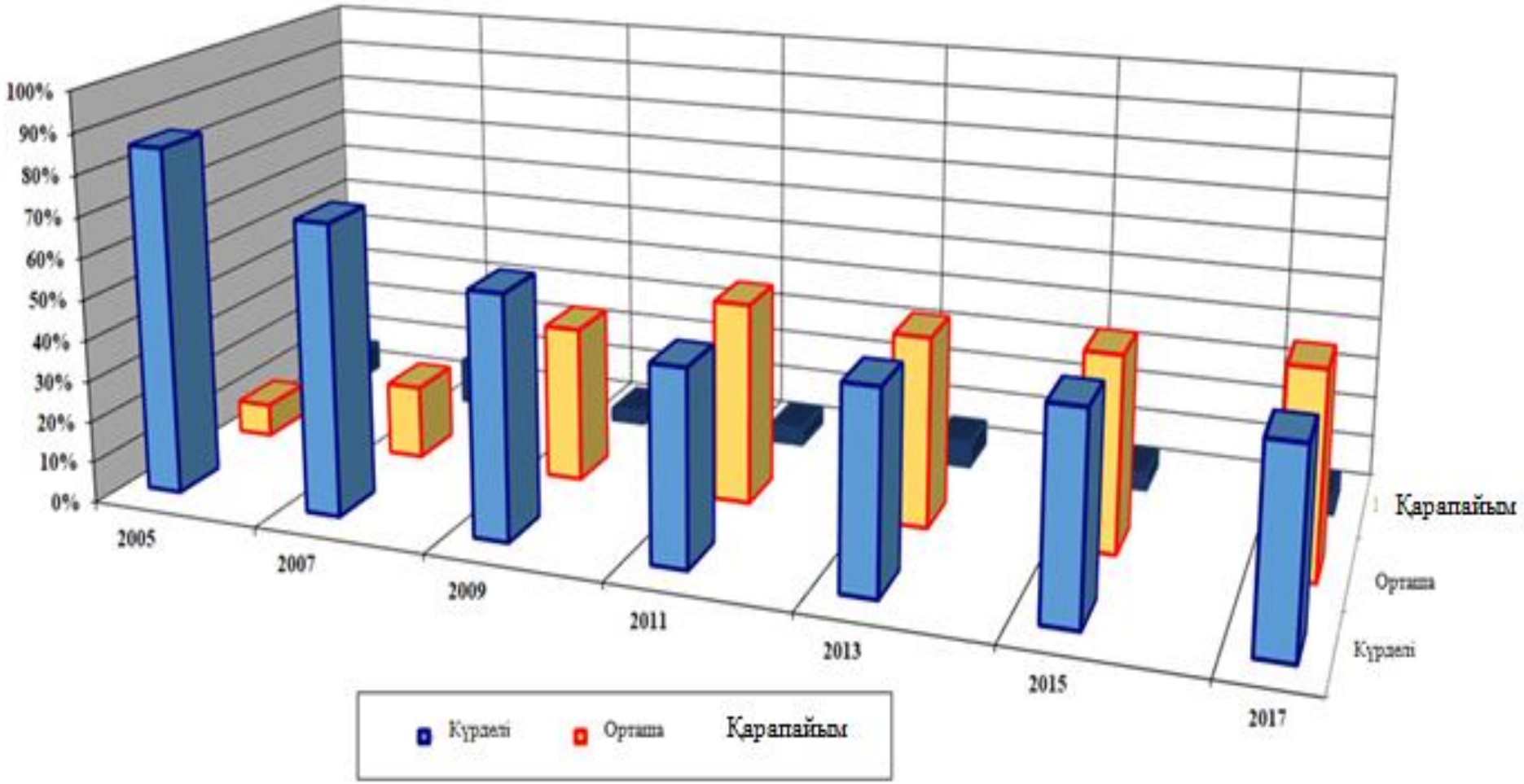
Зерттеу жұмыстарында [28-31] бүгінгі таңда білім беру саласындағы халықаралық инвестициялық жобалар, атап айтқанда, цифрлық ақпараттық-білім беру платформалары халықаралық ынтымақтастықтың әдеттегі тәжірибесіне айналғаны атап өтілді.

Біздің ойымызша, мұндай инвестициялық жобалар міндетті түрде ЖОО-ның және оның ақпараттық білім беру ортасының киберқауіпсіздігін қамтамасыз етудің қаржы стратегияларын терең талдауын болжау қажет.

Ақпаратты қорғау мамандарының айтуынша жоғары оқу орнының КҚ жүйесі, атап айтқанда, ірі халықаралық, мемлекеттік және жеке жоғары оқу орындарының КҚ жүйесі ақпараттық массивтер мен мәліметтердің, оның ішінде құпия мәліметтердің сақталуын қамтамасыз етіп қана қоймай, сонымен қатар ЖОО АББО -ға сырттан рұқсатсыз кірудің мүмкін еместігіне кепілдік беруі тиіс [24,29].

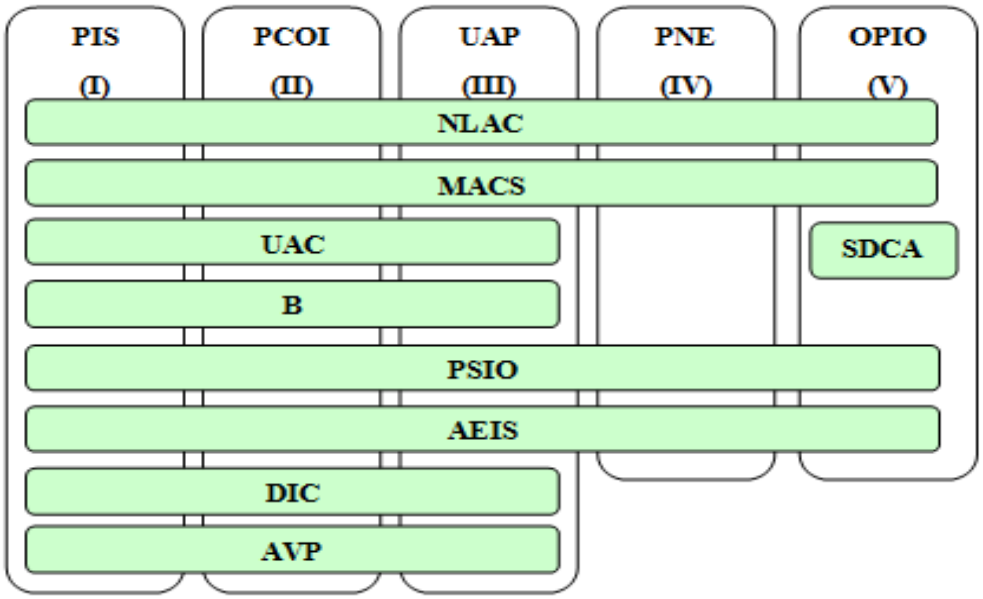
Әлемдегі киберқылмыс санының тұрақты өсуі, атап айтқанда, ЖОО үшін КҚ жүйесіне қаржы салымдарын ұлғайту қажеттілігін көрсетіп отыр [28, с.12].

Әр түрлі авторлардың берген ЖОО АББО туралы түсініктемелері бойынынша және киберқауіпсіздікті қамтамасыз ету міндеттерін ескере отырып ЖОО АББО-ның құрылымын өзгертуге болады [23, с.112]. Осылайша, ЖОО-ның қорғалған АББО-сы және оған сәйкес ақпараттық-білім беру кеңістігінің құрылымы мына түрде ұсынылады (сурет 9).



Сурет 8 - Кибершабуылдардың күрделілік деңгейіне қойылатын талаптардың өсу динамикасы

а) ЖОО АББО кеңістіктері



б) ЖОО АББО кеңістіктерінің КҚ периметрлері және ақпараттық нысандардың сыртқы периметрлері

Қабылданған белгілеулер: AVP – antivirus protection; DIC – data integrity control; AEIS – audit of events of information security; PSIO – physical security of information object; B – backup; UAC – user access control; SDCA – subsystem of detection of cyber attacks; MACS – Monitoring and; analysis of cyber security; NLAC – Network-level access control.

ЖОО АББО КҚ-ның периметрлері: PIS (I) – The perimeter of the information system; PCOI (II) – Perimeter of control of object of informatization; UAP (III) – User Access Perimeter; PNE (IV) – The perimeter of the network equipment; OPIO (V) – The outer perimeter of information object.

Сурет 9 - ЖОО-ның қорғалған ақпараттық білім беру кеңістігінің құрылымы

Әрине, жоғары оқу орнының қорғалған АББО (бұдан әрі- ЖОО ҚАББО) сияқты күрделі ұйымдық құрылымын құру үлкен қаражатты талап етеді және бұл қаражатты жұмсауды сауатты басқару қажет.

Инновациялық жобаларға, атап айтқанда, ЖОО АББО-ны қалыптастыруға баса назар аудара отырып, білім берудің цифрлық технологияларын дамыту саласында инвестициялау процедурасы көбінесе ЖОО-ның киберқауіпсіздігін қамтамасыз ету міндеттеріндегі белгісіздік пен қауіптіліктің жоғары деңгейімен сипатталады. Соңғы жылдары өзгерген киберқатерлердің ландшафты (түрлері) көптеген жоғары оқу орындарының КҚ міндетіне деген көзқарасына түбегейлі әсер етті [26, p.635]. Ең алдымен, бұл ЖОО АББО үшін маңызды потенциалды осалдықтар мен киберқатерлерге, кибершабуылдардың жаңа кластарының пайда болуы, мәліметтерді жеткізудің сымсыз технологияларының кең таралуы және тағы басқа жағдайларға байланысты болды. Білім беруде цифрлық технологияларды қарқынды енгізу жағдайында, мысалы, РФ, Украина, Қазақстанда жеке және ірі халықаралық жоғары оқу орындарын құру кезінде ЖОО АББО-ның киберқауіпсіздігі міндеттеріне көп инвесторлар тиісті көңіл бөле қоймады [23, с.117]. Осы саладағы біраз басылымдарда ғана киберқауіпсіздік жүйесіне ЖОО-ның өзара қаржылай инвестициялауда әртүрлі стратегияларын табуға байланысты модельдердің сипаттамалары бар [11].

Жоғары оқу орнының КҚ жүйесіне енгізілген әр түрлі инвестициялық жобаларды бағалау кезінде нәтижелілікті арттыру және инвестициялауға байланысты шешімдерді қабылдау үшін қазіргі заманғы ақпараттық технологияларды пайдалану қажет. Мысалы, шешімдерді қабалдауды қолдау жүйелерін (ШҚҚЖ) қолдануға негізделген технологиялар [12].

ШҚҚЖ-ның ақпараттық-алгоритмдік компонентін толтыруды ЖОО КҚ жүйесін инвестициялау үшін математикалық модельдерге арналған алгоритмдер блоктарды енгізу арқылы жүзеге асыруға болады.

Әр түрлі ақпараттандыру нысандары (бұдан әрі АН, ақпараттандыру нысандары: ЖОО АББО-сы, күрделі өндірісті басқарудың автоматтандырылған жүйесі немесе банк жүйесінде болу мүмкін) үшін КҚ бойынша міндеттердің ортақтығына қарамастан, олардың әрқайсысының киберқатерлеріне байланысты өзіндік ерекшеліктері бар екенін атап өтеуге болады [5]. Алайда, кез келген АН-нің тиімді қорғау жүйелерін және КҚ жүйелерін құру кезінде жалпы бастапқы міндет - нақты қорғау нысандарын зерттеу есебі, потенциалды бұзушының (компьютер қаскүнемдері) және киберқатердің модельдерін қалыптастыру [28, с.6]. Жоғарыда көрсетілген қадамдарды іске асыру, сайып келгенде, ЖОО АН-нің және жеке жағдайда ЖОО АББО-ның ақпаратты қорғау жүйелері үшін сай (адекватты) талаптар алуға мүмкіндік береді.

ЖОО АББО үшін кибершабуыл сценарийлерінің күрделенуі жағдайында ЖОО-ның және басқа да оқу орындарының ақпараттық қауіпсіздік қызметтерінің талдаушылары кибершабуылдарға, қатерлер аномалияларына жеткілікті түрде

жедел жауап берулері қажет. Бұл компьютер қаскүнемдері немесе ЖОО- ның жауапсыз қызметкері тарапынан диструктивті араласуға әрекет етуге бағытталған міндеттерінде шешім қабылдау нәтижелілігін арттырудың жаңа тәсілдерін іздестіру есебі өзекті мәселе. Мұндай жағдайда АН-нің киберқорғауын қамтамасыз ету міндеттерінде шешімдерді қабылдауды қолдаудың әртүрлі интеллектуалды жүйелері (ШҚИЖ) және сараптамалық жүйелер (СЖ) маңызды рөл атқара алады [22-24].

КҚ міндеттеріндегі ШҚИЖ-ның және СЖ-ның математикалық компоненті - мамандарға шешімдерді қабылдауды қолдауды интеллектуалдандыруға мүмкіндік беретін әртүрлі модельдер мен алгоритмдер. Зерттеу барысында ЖОО АББО-ның ресурстарына рұқсатсыз қол жеткізудің негізгі түрлері үшін аналитикалық модельдерді синтездеу мүмкіндігі қарастырылды. ЖОО АББО-ның киберқорғау жүйелерінің функционалды модельдерін Петри желісінің теориясы арқылы сипаттау мүмкіндігі болашағы зор болып көрінеді [3]. Мұндай түсінік АҚ және ақпаратты қорғау талдаушыларына қорғалатын ЖОО АББО-дағы қатерлерді нақтылауға мүмкіндік береді. Сондай ақ, болашақта жаңа киберқатерлер алдында АН-нің осалдығын потенциалды сипаттай алатын жағдайды анықтауы мүмкін. Сонымен қатар, бұл модельді әртүрлі АН үшін киберқатерлерді талдау процесінде жобаланатын ШҚИЖ-дың математикалық және алгоритмдік компоненті ретінде Петри (және Петри–Марков) және Петридің боялған желілерін негізге ала отырып қолдану перспективасы қарастырылады. Біздің ойымызша, бұл пайымдаулар біздің жұмысымызды өзекті етеді және әртүрлі АН үшін ақпаратты қорғау және КҚ есептерінде ШҚИЖ-ны құру құру бойынша жұмыстың тиімділігін арттырады.

Демек, ШҚҚЖ үшін КҚ жүйесін қаржыландырудың нақты процестерінің сайлылығын сипаттауға мүмкіндік беретін жаңа математикалық модельдерді құру есебі өзекті мәселе. Бұл жоғары оқу орның КҚ жүйесін қаржыландыру стратегиясын мағынасына жетіп барып таңдауға мүмкіндік береді.

1.3 Оқу орындарының ақпараттық кеңістігінің киберқорғау саласындағы алдыңғы зерттеулерге шолу және талдау

ТМД елдері ғалымдарының көптеген еңбектері мемлекеттік құрылымдардың, оның ішінде ЖОО-ның ақпараттық-коммуникациялық жүйелерінің (АКЖ) киберқорғау міндеттерін теориялық зерттеуге арналған: Р.Н.Акиншин [29], Б.С. Ахметов [12], Р.Г. Бияшев [13], О.В. Есиков [23,29], А.Г. Корченко [4], В.А. Лахно [22], А.А. Малюк [24], А.А.Петров [25], В.А. Хорошко [28], R. Ortalo [26], P. Puhakainen [27].

Алайда, Қазақстанда және ТМД-ның басқа елдерінде бұл басылымдардың мазмұны шектеулі немесе айтарлықтай аз, олар тек «жоғары оқу орындарындарын киберқорғау қажеттілігі» тақырыбындағы баяндамалардың тезистерімен ғана шектелген [13, p.49]. Теориялық нәтижелер мен зерттеу нәтижелері кейбір басылымдарда [21, с.34], эксперименттік мәліметтер немесе

имитациялық модельдеу нәтижелері басқа басылымдарда берілген [4]. Зерттеудің жеке сегменті ЖОО үшін АҚ-ны және КҚ-ны қамтамасыз етудің аппараттық және бағдарламалық құралдарын құру міндеттеріне арналған [3, p.3].

Жарияланымдардың едәуір көп бөлігі, атап айтқанда, ЖОО КҚ жүйесі үшін қаржылай инвестициялаудың тиімді стратегияларын таңдауға арналған зерттеулер [6,8,13].

АҚ және КҚ модельдерінің ішінде Гордон-Лоеб (ГЛ) моделі ең негізгі және кең таралған. Бұл модельдің мақсаты ақпаратты қорғауға инвестициялардың оңтайлы мөлшерін анықтауға байланысты міндеттерді шешу.

ГЛ моделіндегі негізгі жағдай қарастырылып отырған ақпараттандыру нысаны үшін, атап айтқанда ЖОО АББО үшін АҚ-ның және КҚ-ның деңгейін анықтайтын осалдық функциясын енгізу және дамыту. Ақпараттық нысанның әртүрлі формалары болуы мүмкін: қолданушылар тізімі, бухгалтерлік есеп кітабы, стратегиялық даму жоспары, веб - сайт және т.б. Қауіпсіздікті арттыру құпиялылықты, тұтастықты, нақтылықты, сенімділікті, қолданушылардың авторизациясының қол жетімділігін және т.б. қорғау бағытында орын алуы мүмкін.

Модель құрылымы бойынша статикалық болады. Демек, шешімдер мен нәтижелер бір уақытта пайда болады, ал динамикалық әсерлер, оның ішінде қаржының уақытқа тәуелділігі ескерілмейді.

АҚ және КҚ құралдары мен әдістеріне инвестициялар жұмсау осалдықтың жеткілікті кіші және жеткілікті үлкен мәндерінде тиімсіз екенін ескере отырып, ГЛ моделінің авторлары, сондай-ақ ГЛ моделіне негізделген идеяларды дамытқан [30] бірқатар жұмыстарда келесі жағдайлар атап өтілген.

Көптеген авторлар нысандарды төмен, орташа және жоғары осалдық деңгейлеріне бөлуді басқарудың бірінші міндеті және бұл жобалаудың алғашқы кезеңдерінде жасалуы керек деп санайды. Алайда, ГЛ моделінің және оған ұқсас модельдердің авторлары оның кемшіліктерін атап өтті:

– Шабуыл ықтималдығын және ақпараттық массивтердің осалдығын анықтайтын қарапайым процедура жоқ.

– Ақпараттандыру нысанының қорғау периметрлерінің қауіпсіздігі мен киберқауіпсіздігінің бұзылуынан болатын потенциалды шығындарды анықтау қиынға соғады. (ЖОО АББО үшін бұл АҚ және КҚ периметрлері әлі де жеткілікті түрде шартты екенін ескереміз).

– Зерттеу нәтижелерін белгілі бір нысанға қатысты іске асырудың күрделілігі.

– Шабуылдаушының қорғаныс үшін қосымша инвестициялар салу кезінде өз стратегиясын қалай өзгертетіні ескерілмеген, атап айтқанда, динамикалық режимде қарама-қарсы келудің талдауы жоқ.

ГЛ моделі кеңінен танылып және жарияланған кезден бастап он жыл ішінде көптеген жұмыстарда дамытылғанына қарамастан, қойылған сұрақтардың басым

бөлігі бүгінгі күнге дейін шешілмеген болып отыр. Модель авторларының сөзсіз еңбегі - бұл міндетті алғаш рет мұқият қарастырып және осалдық функциясын анықтағаны, ақпараттық саладағы қарама - қарсы тұруды қарастырудағы басты мәселе. Функцияның түрін анықтау, динамикалық жүйенің осалдығын білдіреді, ақпараттық қарама- қарсы тұруды математикалық модельдеудегі басты мәселе және көптеген зерттеушілердің жұмыстары осы мәселеге арналды [31].

Егер біз міндеттің тарихына жүгінетін болсақ, онда екі тараптың қарама-қарсы тұруын бірінші рет екінші дүниежүзілік соғыстың соңында әскери жоспарлаудың математикалық негіздерін құру кезінде RAND Corporation мамандары мұқият қарастырды. RAND фирмасы жасаған екі тараптың қарсы тұру моделі тактикалық әскери операцияларды имитациялауға арналған Гросс моделі [15]. Осы модельге сәйкес, қақтығысушы тараптардың X және Y ресурстары бар, олардың қарама- қарсы тұру нәтижесі салынған ресурстардың айырмашылықтарына сызықтық тәуелді және сызықтық бағдарламалар есебіне әкелетін мақсатты функциямен анықталады.

Әскери операцияларды жоспарлау кезінде пайда болған Гросстың есебінің қарастырылған есептерден бірқатар айырмашылықтары бар. Біріншіден, мақсатты функция дискретті, өйткені қорғаныс арқылы өтудің немесе шабуылды жоюдың немесе қорғаныс санын анықтайды. Екіншіден, бұл өлшемдер қарама-қарсы күрестің әрбір эпизодында шабуылдаушы үшін де және сәйкес қорғанушы үшін де бірдей.

Нысандардың біртектілігі есепті шешуді айтарлықтай жеңілдетеді, алайда қарсы күресу шарттарын шектейді. Алайда, Гросс моделінің басты кемшілігі - оның мақсатты функциясының сипаты үзік - сызықтық болып табылуында, ол әрине, нақты жағдайларға сәйкес келмейді. Осы себепті Гросс моделін оның қарапайымдылығын ескере отырып, мақсатты функцияны аппроксимациялау және бірінші жуықтауда нәтижелерді алу үшін ғана пайдаланады [22].

Ақпаратты қорғауға арналған шығындар көлеміне және КҚ-ға байланысты, қатерлерді іске асыру салдарынан болған шығындар деңгейін есептеуге мүмкіндік беретін тағы бір математикалық модель модельдер [17,19] жұмыстарда сипатталған. Мына зерттеу жұмыстарының [21,30] мақсаты, ықтимал бөлудің белгілі әдістерін қолдана отырып, ақпаратты техникалық қорғау кешенінің (АТҚ) тұрақтылығын бағалау болды.

Қорғауға немесе оны модернизациялауға қаржылай инвестициялар болмаған жағдайда, уақытқа қарамастан қорғалудың сенімділігі нөлге тең болады. Бұл модель қамтамасыз ету ықтималдығының неғұрлым тиімді қаржыландыруға тәуелділігін анықтауға мүмкіндік береді.

Модельді құрудағы негізгі қиындықтар бұзу нәтижелері туралы статистикалық мәліметтерді жинаумен байланысты (және қорғаудың бұзылу фактісінің қажеттілігі), өйткені мұндай қорғаныс жүйесі бұдан кейін қайталанып қолданылмайды. Осыған байланысты автор [9,12] жеке қорғаныс жүйелерінің

ықтималды сенімділігін бағалауға және оны бірнеше нысандарға орнатуға мүмкіндік беретін нақты бұзу әрекеттері негізінде АТҚ-ның ықтималды сенімділігін анықтау әдісін жасады (мысалы, бірнеше компьютерге антивирустық бағдарламаны орнату әрекетті ғана емес, сонымен қатар басқа компьютерлерді бұзу мүмкіндігіне кететін уақытты да қарастыруға болады) [10,16]. Бұл әдістің кемшілігі- бұл жағдайда жүйенің нақты бұзылуы салдарын талдау нәтижесінен алынатын АТҚ-ның тиімділігін білу қажеттілігі.

Зерттеулер нәтижесінде [29,31], авторлар АТҚ қасиеттерін анықтайтын параметр тек тұрақты шама ғана емес, сонымен қатар функция да да бола алатындығын көрсетті. Сонымен қатар, бұл функция бұзу әрекеттеріне және мұндай әрекеттер орын алған уақытқа байланысты тәуелді болады, мысалы, ақпараттандыру нысанының желісінде қолданушыны аутентификациялау процедурасы барысында парольдерді таңдау тактикасы кезінде [18,22]. Зерттеу нәтижелері бойынша, бұзу әрекеттерінің жиілігін есептеуге мүмкіндік беретін функциялар алынды.

Глушак-Новиковтың моделі [50] қорғаудың максималды деңгейін қамтамасыз ететін жүйенің компоненттері (нысандары) арасында қорғаныс механизмдерін оңтайлы орналастыруға бағытталған.

Ақпаратты жоғалтудың минималды тәуекелін қамтамасыз ететін қорғау механизмдерінің оңтайлы жиынтығын іздеу, аумақтық таратылған ақпараттандыру нысанның аудандық бөлімшелерінің жүйесі мысалында жүргізілген (автор банк бөлімшесінің мысалында қарастырды) [34, p.155]. Әрбір бөлімшедегі ақпарат көлемі потенциалды клиенттердің саны, атап айтқанда аудан тұрғындарының санына пропорционалды. Жекелеген қатерлерді іске асыру ықтималдығы, сондай-ақ қорғау механизмдерінің әрқайсысының құны мен тиімділігі сараптамалық бағалау әдісімен анықталады. Бұл жағдайда әрбір нысан үшін қатердің туындау ықтималдығы бірдей және тек қатердің түріне байланысты болады деп болжанады. Әрбір аумақтық бөлімшелер үшін қорғаныс элементтерінің әртүрлі комбинацияларын ескере отырып, бүкіл жүйеге келтірілген жалпы барлық шығындар (ол қауіптің дәрежесін сипаттайды) және әрбір бөлімше үшін қорғаныс элементтерінің оңтайлы жиынтығы есептеледі. Сонымен бірге қорғау жүйесінің жалпы құнына шектеулер енгізу шарттарын тексеру қарастырылған.

Толық қауіпті есептеу кезінде әртүрлі қатерлерді жүзеге асырудан болатын шығын мөлшерін көрсететін теңдеулердің қиылысқан мүшелерінің мәні туралы міндет ашық күйінде қалады (бұл оқиғалар үйлесімді болып саналады) [7,p.889].

О.Е.Архиповтың жұмыстары тәуекелдерді бағалау және ақпараттық қауіпсіздікке салынған инвестициялардың тиімділігін зерттеу үшін «шабуыл-қорғау» экономикалық-құндық модельдерін қолдану міндеттеріне арналған [32]. Осы модельдердегі тәуекелдің ықтимал параметрлерін анықтау үшін ақпарат саласындағы «шабуыл-қорғау» жағдайына тән мотивациялық- құндық және

экономикалық-қаржы қатынастардың белгілі бір сипаттамалары қолданылады. Атап айтқанда, шабуылдаушы А (шабуылдаушы) кейбір I ақпараттық ресурстарға қатысты Т қаупін жүзеге асырған кезде пайда болатын жағдай В тарабына тиесілі.

Ақпараттық қатерді жүзеге асырудың экономикалық және шығындық сипаттамаларын талдау мен сандық бағалаудың нақты мүмкіндігі болған жағдайда, авторлар [33-36] еңбектерінде келтірілген модельдерді кез-келген нақты ұйымның тәуекелдерін есептеу үшін қолдануды ұсынады. Осы бағалаудың нәтижесін белгілі бір қосымша ақпарат болған кезде тәуекелдер менеджменті стандарттарының параметрлері мен ұсыныстарына сәйкес ұйымның ақпараттық қауіпсіздік жай-күйін зерттеу (аудит) жүргізу арқылы алуға болады, уақыт бойынша статикалық бағалауды қабылданған экономикалық-құндық шабуылдарды дамыту сценарийлеріне сәйкес уақыт өте келе өз мәндерін өзгертетін динамикалық түрде дамытуға болады [13].

«Шабуыл-қорғау» экономикалық-құндық модельдері нақты ұйым туралы нақты ақпарат негізінде осы ұйымның ақпараттық қауіпсіздігіне салынған қаражат көлемі жағынан жеткілікті ме екенін тексеруге мүмкіндік береді [33].

Ақпараттық жүйелерге жасалған кибершабуылдарды зерттеу В. А. Хорошконың [28] жұмыстарында көрсетілген. Кибершабуылдар кезінде қаскүнемдердің мүмкіндіктерін бағалау талдаудың ойын әдістерін пайдалана отырып жүргізіледі [37].

Ақпараттық салаға кибершабуылдаудың оңтайлы циклын рәсімдеу (шартты таңбалардың көмегімен модельді жазу) кезінде В.Нэш тұжырымдамасы қолданылады деп болжануда [49,57]. Бұл модельде қаржыландырудың оңтайлы шешімді таңдауға әсері ескерілмегенін айта кету керек, алайда зерттеушілер құрған талдаудың ойын әдістері жеке және топтық кибершабуылдарды бағалауға мүмкіндік беретінін көрсетіп отыр. Бұл ақпарат саласына мысалы, оқу орындарына жасалған кибершабуылдардан ақпараттың қорғалу деңгейінің кепілдендірілген және сенімді бағаларын алуға мүмкіндік береді [36].

Экономикалық қатынастар мен ақпараттық саланың, атап айтқанда білім беру саласының дамуы бәсекелестіктің күшеюіне, ақпарат көлемі мен құнының артуына, сондай-ақ ақпараттың жайылып кетуінен болған потенциалды шығындардың артуына, ақпараттық нысандар санының өсуіне (бұл әсіресе ЖОО АББО-да байқалады және қарқынды) және кибер-инциденттердің жиі болуына әкеледі. Бұл ретте екі тараптың: ақпаратты қорғау мен шабуылдаушы- қарама – қарсы тараптардың динамикалық өзара әрекеттесуін көрсете отырып, қарсы тұру жағдайларының шарттары да үнемі өзгеріп отырады.

Киберқорғау тараптарының стратегиясы мен тактикасының өзгеруі ақпараттық ресурстарға жаңа шабуылдар тудырады, олар бір жағынан қарсыластың ниетін көрсетеді, екінші жағынан шабуылдар немесе деструктивті араласудың өзге де әрекеттері бағытталған қорғаныстың әлсіз жақтарын көрсетеді.

ЖОО АББО-дағы КҚ-ны және АҚ-ны қамтамасыз ету тәсілдеріндегі өзгерістердің басқа себептері ақпараттың «ескіруіне», жаңа ақпарат пен қосымша ресурстарды енгізілуіне, нысандар арасында ақпараттық ресурстарды қайта бөлуге, олардың арасындағы жаңа байланыстардың пайда болуына байланысты факторлар болуы мүмкін.

Ақпараттық саладағы екі тараптың антагонистік қарсы тұруы , әдетте қорғаушыға шабуылдаушының (хакердің) іс - әрекеттері мен қаржылай мүмкіндіктері белгісіз болғанымен сипатталады.

Сонымен қатар, шабуылдаушылар қорғаныс жүйесінің құрылымы туралы біраз түсінікке ие және қауіпсіздік жүйесінің ең әлсіз буындарын бұзуға өз күш-жігерін жұмсай алады. Бұл шабуылдаушыға өте тиімді.

Қауіп- қатерлердің әртүрлі түрлерін бұғаттауға қорғау ресурстарын бөлу белсенді режимде - қарсыластың іс- қимылының алдын ала отырып, сондай-ақ мүмкін шабуылдардың бағыты айқын болған кезде қаржыландыруды кешіктіріп, атап айтқанда бейімделіп жүргізілуі мүмкін.

Ресурстарды динамикалық басқару қажеттілігі келесі себептерге байланысты:

– қарсыластың іс- әрекеті нұсқаларының белгісіздігі, атап айтқанда, ақпаратты алуға бағытталған күш-жігерінің бағыты және осы жұмыстың ауқымы, атап айтқанда бұзуға жұмсаған хакерлердің ресурстарының қаржы компоненттеріне де байланысты;

– уақыт өте келе қарама-қайшылықтың ішкі және сыртқы жағдайлары-ақпарат құнының өзгеруімен, оның нысандар арасында бөлінуімен, қарсыластың шабуылдарының бағытының өзгеруі, жаңа шабуылдаушылардың пайда болуымен;

– ақпараттық жүйе күйінің өзгеруі (ЖОО АББО-сы дербес жағдай ретінде қарастырылады), атап айтқанда, шабуылдардың бағытын анықтағаннан кейін және қорғау тарапынан тиісті шаралар қабылдағаннан кейін оның ең әлсіз буынының өзгеруімен.

Ақпаратты қорғау жүйелерін математикалық моделдеу бойынша ғылыми жұмыстарды талдау, негізгі міндет қорғауды қаржыландырудың көлемін анықтауға бағытталғанын көрсетті (кесте 2).

Қаржыны қорғау нысандары арасында бөлу міндеттері кейбір жұмыстарда көрсетілген [34, 59]. Сонымен қатар, қолданыстағы нәтижелер (модельдер) [35,58], шабуылдаушының мүмкін әрекеттері мен олардың салдары жүйенің көрсеткіштері мен сипаттамаларының өзгеруіне әсерін тигізетіні сирек ескереді.

Осылайша, зерттеліп отырған тақырыптағы жұмыстарға жүргізілген талдау шаруашылық қызмет субъектілері мен оқу орындарының ақпаратын қорғау үшін шектеулі қаржы ресурстарын тиімді пайдалану міндеті аса маңызды және маңызды бола түсетінін көрсетті [27].

Кесте 2- Ақпараттандыру нысандарының ақпараттық қауіпсіздігіне және киберқауіпсіздігіне инвестициялаудың математикалық моделдерінің салыстырмалы сипаттамасы

Салыстырылатын критерилер / Моделдер	**Қорғаушының ресурстары ескерілді**	**Шабуылдаушының ресурстары ескерілді**	**Қорғаныс құралының құны ескерілген**	**Нысандардың осалдығы ескерілді**	**Қорғау нысандары арасында ресурстарды бөлуді оңтайландыру**	**Динамикалық режимде оңтайлы шешімді есептеу**
Гросс	+	+	-	-	+	-
Гордон-Лоеб	+	-	-	+	-	-
Задирак	+	-	-	-	-	-
Глушак –Новиков	+	-	+	-	+	-
Журиленко	+	-	-	+	-	+
Архипова	+	+	+	+	-	+
Хорошка	-	-	-	+	-	+

Сонымен қатар, шабуылдаушы тараптың іс- әрекеттері мен қаржы ресурстарын белгілі бір ықтималдықпен ғана болжауға болатын белгісіздік жағдайында, теориялық-ойын әдістерін пайдалану және қарама-қайшылық шарттарының өзгеру динамикасын ескере отырып қорғау нысандары арасында шектеулі ресурстарды оңтайлы бөлуді іздеу ақпараттың жайылып кетуінен болған қаржылай шығындарды барынша азайтуға мүмкіндік береді.

Компьютерлік жүйелер мен ақпараттық технологиялардың дамуы КҚ жүйесін инвестициялауды оңтайландыру бойынша жұмыстардың жеке тұжырымдамасын тудырды. Зерттеудің бұл тұжырымдамасы КҚ саласындағы инвестициялаудың рационалды стратегияларын анықтау есептерінде сараптамалық жүйелерді (СЖ) [2] және ШҚҚЖ –ны [6] кеңінен қолдануға негізделген. Біз осы салада көптеген жұмыстарды зерттеп, осы жарияланымдардың көпшілігінде [5,8,12] жоғары оқу орнының КҚ жүйесін өзара қаржылай инвестициялаудың рационалды стратегиясын таңдау бойынша нақты шешімдерді қарастырмаған деген қорытындыға келдік.

Сонымен қатар, [9] және [10] жұмыстарының қорытындыларында КҚ-ны инвестициялауды басқарудың рационалды стратегияларын таңдау процедураларын автоматтандыру үшін СЖ-ны және ШҚҚЖ-ны қолдану кезінде

нақты ұсыныстар берілмеген. Бұл жағдайлар жоғары оқу орнының КҚ жүйесін өзара қаржылай инвестициялаудың рационалды стратегияларын анықтау есептерінде ШҚҚЖ үшін жаңа модельдерді құру қажеттілігімен байланысты міндеттің туындауына себепші болды. Осы тақырып бойынша жасалған зерттеулердегі [13, 61] авторлардың баяндаған тәжірибе мен тәсілдеріне, сондай-ақ зерттеу әдістемелері ұқсас авторлардың жұмыстарына [15,68] сүйене отырып, осындай міндеттер класын шешуде жеткілікті тиімді тәсіл: бірнеше терминалды беті бар дифференциалдық сапа ойындары теориясының әдістерін қолдану деп айта аламыз [17,18]. Осылайша, осы тақырып бойынша зерттеулерге жүргізілген талдау жоғары оқу орнының КҚ жүйесін үздіксіз өзара инвестициялау есептерінде ШҚҚЖ үшін модельдерді одан әрі дамыту міндетінің өзектілігін растады. Бұл тұжырым инвесторлар үшін нақты ұсыныстар құру қажет болған кезде өте маңызды. Бірақ күрделі математикалық есептеулерді қолданудың қажеті жоқ, себебі есептеулердің көп бөлігі компьютерлік бағдарламалармен орындалады.

Мына жұмыстарда [19, 81] АН-нің КҚ қатерінің моделін сипаттау үшін Петри желілерін қолдануға арналған зерттеулердің нәтижелері келтірілген. Бұл жұмыстар осы міндетінде айтарлықтай теориялық үлес қосса да, біздің ойымызша, авторлар ұсынған модельдерді, атап айтқанда АН-ді ақпаратты қорғау және КҚ бойынша ШҚИЖ-да және СЖ-да бағдарламалық жүзеге асыру (программалау) біршама қиынға соғады.

Мына зерттеу жұмыстарына [25, 69] сүйене отырып, қатерлердің модельдерін АН-нің қорғалуын бағалау міндетін өзектендіру кезінде қатерлерді көрсетудің көрнекі кестелік формасын қолдана отырып құруға болады. Бірақ жоғарыда көрсетілгендей, бұл тәсілмен қатерлердің моделін жасау көп еңбекті қажет етеді. Сонымен қатар, қатерлер санының өсуі, әсіресе КҚ саласында жұмыс тәжірибесі аз мамандар үшін мұндай кестені құрды қиындатады.

Петри (Петри–Марков) желілері шабуылдаушының модельдерін сипаттау үшін де сәтті қолданылды [70]. Алайда, авторлар шабуылдаушының моделін нақтылау мүмкіндігін, атап айтқанда, оны графтар теориясының негізінде құрылған модельдермен біріктіру арқылы нақтылау мүмкіндігін қарастырмады, бұл нақты АН үшін киберқорғау периметрлерінен (шекарасы) шабуылдаушының еңсеру процесіндегі күйлердің ауысуын дәлірек сипаттауға мүмкіндік берер еді.

Зерттеулерде [71-77] әр түрлі АН үшін ақпаратты қорғау жүйесінің модельдері Петри желісінде алдын ала іріктелген қарапайым операциялардың тізбегі ретінде қарастырылған, олардың ішінде кибершабуыл да болуы мүмкін. Модельдер берілген уақыт аралығында әртүрлі шабуылдардың жүзеге асу ықтималдығын есептеуге мүмкіндік береді. Алайда, [80,82,83] зерттеулерде қарастырылған модельдер жаңа киберқатерлерді жүзеге асыру процесінде уақытқа байланысты сипаттамаларды есептеуге мүмкіндік бермеді.

Зерттеулерде [84,85] Петри желілеріне негізделген және ақпараттық жүйелерде (АЖ) қатерлерді іске асыру процестерін сипаттайтын және модельдер

ұсынылды. Бұл модельдер АН-ді қорғаудың көптеген параметрлерін атап айтқанда, қатерлердің орындалу ықтималдығын, қатерлердің орындалу уақытын бағалауға мүмкіндік бергеніне қарамастан, шабуылдаушының іс- қимылдарының реті соңына дейін толық аяқталмаған. Атап айтқанда, бұл жұмыстарда әртүрлі кластарға жататын шабуылдар барысында АЖ-ның жай- күйінің өзгеруі кезінде туындайтын қақтығыс жағдайларды шешу міндеті зерттелмеген. Бұл жағдай, біздің ойымызша, осы зерттеулердің практикада қолданылуына шектеу болады.

Осылайша, қатерлерді анықтау мен талдаудың қолданыстағы әдістерін, Петри желілерін алгоритмдеу және визуализациялау негізінде шабуылдаушылардың модельдерін толықтыру нақты АН үшін қорғалу жағдайы мен жаңа қатерлерді болжаудың тиімді құралы бола алады. Бұл жаңа киберқатерлердің негізі қайда жатқанын және қандай салдар әкелетінін ұғуға мүмкіндік береді және болашақта әртүрлі ақпараттандыру нысандарының киберқауіпсіздігі мен ақпаратты қорғау қызметтерінің талдаушылары ұсынған тәсілдерді тиімді қолдануға болады.

Бірінші тарау бойынша қорытындылар және зерттеу міндеттерінің қойылымы

Бірінші бөлімде:

– заманауи ЖОО-ның қауіпсіз ақпараттық білім беру ортасын қалыптастырудың алғышарттары қарастырылған. Отандық және жетекші шетелдік зерттеулердің жарияланымдары талданды;

– оқу орындарының ақпараттық кеңістігін киберқорғау саласындағы алдыңғы зерттеулерге шолу және талдау жасалды. Осы тақырып бойынша шыққан жарияланымдарға талдау жасалды. Жасалған талдау жоғары оқу орындарының КҚ жүйесін үздіксіз өзара инвестициялау міндеттерінде ШҚҚЖ үшін модельдерді одан әрі дамыту проблемасының өзектілігін растады;

– ақпараттандыру нысандардың КҚ қатерлерінің моделін сипаттау үшін Петри желілерін қолдануға арналған зерттеулер нәтижелері бойынша жарияланымдарға талдау жасалды. Бұл жұмыстар осы міндетте айтарлықтай теориялық үлес қосса да, біздің ойымызша, авторлар ұсынған модельдерді, атап айтқанда АН-ді ақпаратты қорғау және КҚ бойынша ШҚИЖ-да және СЖ-да бағдарламалық жүзеге асыру біршама қиынға соғады. Бұл өз кезегінде қосымша зерттеулерді талап етеді.

Зерттеу мақсатына жету үшін келесі міндеттерді шешу қажет:

– ЖОО АББО-ның киберқауіпсіздік жүйесіндегі инвестициялық процесс параметрлерінің әртүрлі қатынастарын ескере отырып инвестициялауды басқару стратегияларын табу бойынша шешімдерді қабылдауды қолдау жүйесі үшін модель құру;

– «ЖОО-ның киберқауіпсіздік жүйесінде инвестициялауды басқару стратегияларын табу бойынша шешімдерді қабылдауды қолдау жүйесі» компьютерлік бағдарламасын құру;

– модельдің сайлылығын тексеру мақсатында инвестициялаудың әртүрлі стратегиялары үшін компьютерлік модельдеуді орындау;

– Петри желілерінің аппаратын қолдана отырып, ақпараттандыру нысанының киберқорғауын бейімделген басқарудың тұжырымдамалық моделін құру;

– ЖОО АББО-ның компьютерлік желілерде қолданушының есептерін бөлу моделін құру (ЖОО АББО-ның мысалында);

– ЖОО АББО-ға қол жетімділік құқығын салыстыру тұрғысынан қол жетімділік құқығын бақылау әдістерін толықтыру.

2 ЖОҒАРЫ ОҚУ ОРЫНЫНЫҢ КИБЕРҚАУІПСІЗДІК ҚҰРАЛДАРЫН ҚАРЖЫЛАНДЫРУ БОЙЫНША ШЕШІМДЕРДІ ҚАБЫЛДАУДЫ ҚОЛДАУ МОДЕЛЬДЕРІ

2.1. Жоғары оқу орнының ақпараттық білім беру ортасының киберқауіпсіздігін қаржыландыру стратегияларын талдау

Ақпаратты қорғау бойынша көптеген мамандар атап өткендей, білім беру мекемелерінің, атап айтқанда, жоғары оқу орындарының ақпараттық қауіпсіздік жүйелері және киберқауіпсіздік жүйелері ақпараттық массивтер мен мәліметтердің, оның ішінде құпия мәліметтердің сақталуын қамтамасыз етіп қана қоймай, сонымен қатар оқу орындарының АББО жүйелеріне сырттан рұқсатсыз кірудің мүмкін еместігіне кепілдік беруі тиіс [38]. Жоғары оқу орынының АББО-дағы АҚ-ны және КҚ-ны қамтамасыз ету жөніндегі іс- шаралар сөзсіз қаржы салымдарын қажет етеді [39].

Диссертациялық жұмыстың 1- тарауында көрсетілгендей, сондай-ақ [40,41] зерттеу жұмыстарын ескере отырып, қорғалатын мәліметтерге ЖОО АББО-да сақталатын және қолданылатын мәліметтердің ішінде мыналарды жатқызуға болады, студенттердің, оқытушылардың, ғылыми қызметкерлердің, қызмет көрсетуші персоналдардың жеке мәліметтері; оқу мекемесінің интеллектуалды меншігі болып саналатын цифрланған ақпарат; оқу процесін қамтамасыз ететін ақпараттық массивтер (мысалы, мультимедиялық контенттер, мәліметтер базасы, оқыту бағдарламалары) (кесте 3).

Бұл ақпаратты студенттердің және қызметкерлердің тарапынан болатын бұзақылық оймен немесе сырқы (ішкі) компьютер қаскүнемдері тарапынан ұрлауға немесе бүлдіруге жататын нысан деп қарастыруға болады.

Белгісіздік (қатерлердің белгісіз) жағдайында ЖОО-ның ақпараттық-білім беру ортасын (ЖОО АББО) немесе ЖОО-ның ақпараттық-коммуникациялық жүйелерін (ЖОО АКЖ) қорғаудың тиімді жүйесін құру үшін маңызды міндет қорғау нысандары арасында қаржы ресурстарын бөлудің мүмкін нұсқаларын зерттеу және олардың арасында оңтайлы нұсқасын таңдау. Қорғаушы тараптың мақсаты қатердің орындалу ықтималдығын азайту. Шабуылдаушы қарама- қайшы мақсатты көздейді: ақпараттық қатерлерді іске асыру үшін барынша максималды мүмкіндіктер жасалатындай ресурстарын бөлу. Атап айтқанда, екі тараптың қарсы тұруы туралы айтуға болады [40].

Әрбір тараптың ұтысы қарсыластың стратегиясына байланысты және өзінің мақсатты функциясымен анықталады. Жоғарыда айтылғандардың барлығы атап айтқанда, ЖОО АКЖ-да ақпараттық қауіпсіздік және киберқауіпсіздік қызметтері тарапынан оңтайлы қаржы стратегияларын таңдау міндеттерінде шешім қабылдауды қолдауд интеллектуалды жүйелері үшін жаңа модельдерді жасау бойынша зерттеу проблемаларының өзектілігін анықтайды.

Кесте 3- ЖОО АББО киберқауіпсіздігін қамтамасыз ететін қаржы стратегияларын таңдау үшін қарастырылатын қатерлер тізімі

Қатерлер	Орындалу салдары
WEB сервер жұмысын бұғаттау	Студенттер мен қызметкерлердің ақпаратын ашу немесе түрлендіру
АЖ-ның жұмысын бұғаттау	Студенттер мен қызметкерлердің ақпараттарын ашу, түрлендіру немесе жою
Қызметтік сервердегі ақпаратты жою	Коммерциялық ақпаратты ашу, түрлендіру немесе жою
Құжат айналымы жүйесінде, атап айтқанда берілгендер қоры (БҚ) серверінде ақпаратты жою	Ғылыми жобалар және оларды іске асыру нәтижелері бойынша ақпаратты ашу, түрлендіру немесе жою

Кибершабуылдардың күрделілігінің өсу тенденциясы ақпаратты қорғаудың әр түрлі қолданбалы аспектілері мен барлық ақпараттық жүйелер мен технологиялардың киберқауіпсіздігінде шешімдерді қабылдауды қолдау саласындағы есептеуді интеллектуализациялауміндеттеріне арналған зерттеулер толқынын тудырды, атап айтқанда ЖОО АКЖ-да [20,41]. Сонымен қатар, ақпаратты қорғау құралдарына (АҚҚ) және әртүрлі ақпараттандыру нысандарының киберқауіпсіздігіне, атап айтқанда ЖОО АКЖ-ға инвестициялау стратегияларын таңдау туралы шешім қабылдауды қолдау үшін жаңа әдістер мен модельдерді синтездеуге байланысты жұмыстар жалғасуда. Зерттеу жұмыстарында [42,43] киберқауіпсіздікті қаржыландыру бойынша шешім қабылдау – үздіксіз есеп екендігі көрсетілген. Сонымен бірге, осы зерттеу сегментіндегі бірқатар соңғы жұмыстардың [44-47] талдауы көрсеткендей, олардың жалпы кемшілігі – ЖОО АКЖ-сы үшін ақпаратты қорғау құралдарын және киберқауіпсіздікті қаржыландыру стратегияларын алудың жалпыланған әдістемелерінің болмауы. Бұдан басқа, КҚ-ны инвестициялау стратегиясын сипаттайтын модельдерде [44] шабуылдаушы тараптың қаржы стратегиялары бойынша мәліметтері белгісіз болған жағдайлар туралы айтылмаған. Зерттеу жұмыстарында [38-41] ұсынған модельдер киберқорғау тарапының қаржы ресурстарын жоғалту тәуекелін бағалауға мүмкіндік бермейді. Біздің ойымызша, ЖОО АКЖ-да АҚҚ мен КҚ құралдарын қаржыландыру стратегияларын оңтайландыру міндетіндегі көптеген тәсілдердің кемшіліктерін дифференциалды және көпқадамды сапа ойындар теориясының әдістерін қолдану арқылы жоюға болады [45]. Зерттеу жұмыстарында [46,47] оқу орындарының ақпараттық-коммуникациялық жүйелерін қарқынды цифрландыру және жаһандандыру жағдайында жоғары оқу орнының АББО-да сенімді және тиімді қорғауды қамтамасыз ету міндетінің маңыздылығы көрсетілді [48-52]. Ірі ЖОО мен білім беру платформаларында да киберқауіпсіздікте болатын әртүрлі «әлсіздіктер»

периодты түрде кездеседі [51]. Осылайша, ЖОО АББО-да КҚ жүйесін қаржыландыру есебі үздіксіз. Білім беру саласын жаһандандыру және цифрландыру дәуірінде ЖОО АББО-да КҚ жүйесін қаржыландыру тиімділігін бағалау міндеті қазіргі заманғы білім беру мекемелерінің, атап айтқанда жоғары оқу орындарының киберқауіпсіздік және ақпаратты қорғау қызметтері үшін басым бағыттардың бірі. Бұл зерттеу тақырыбына, тек соңғы жылдарда ғана көптеген жарияланымдар арналған [10,34,42]. Көптеген жұмыстардың кемшіліктері ЖОО АББО-да КҚ жүйесін қаржыландыру стратегиясын құру бойынша нақты ұсыныстардың болмауы. Атап айтқанда, бұл шабуылдаушы тарапқа белсенді қаржылай қарсы іс-қимылды модельдеу міндеттеріне байланысты аспектілерге де қатысты. Зерттеу барысында ЖОО АББО-да КҚ жүйесін қаржы стратегияларын таңдау үшін әр түрлі сараптамалық [23] және шешім қабылдауды қолдау жүйелерін [41] қолдануға арналған жұмыстар қарастырылды. Зерттеу жұмыстарында [51-53] сипатталған көптеген модельдер күрделі ақпараттандыру нысандарын, атап айтқанда жоғары оқу орнының КҚ құралдарын қаржыландырудың тиімді ұсыныстары мен стратегиясын табуға мүмкіндік бермейтінін атап өту керек. Зерттеулерде келтірілген нәтижелер [34] ЖОО-ның қорғаушысы шабуылдаушы тараптың ЖОО АББО-ны бұзу үшін жеткілікті қаржы ресурстары болған жағдайда киберқауіпсіздік жүйесіне инвестициялаудың рационалды қаржы стратегияларын қалай құруы керек екендігі туралы нақты жауап бермейді. Зерттеу жұмыстарында [35,42] ЖОО-ның қорғаушысы өзінің қаржы ресурстарын дұрыс пайдаланбаған жағдайларға талдау жеткіліксіз жасалған.

Зерттеу жұмыстарында [45,23] айтылған міндеттермен пікір таласуға болатынын ескере отырып, ЖОО АББО-дағы КҚ жүйесін қаржыландыру есептерінде шешімдерді қабылдауды қолдау интеллектуалды жүйесі (ШҚҚИЖ) үшін модельдерді одан әрі дамыту міндеті өзекті болып қала береді.

Осылайша, жүргізілген зерттеулерге жасалған талдау көрсеткендей, ЖОО АКЖ-да ақпаратты қорғау құралдарын және КҚ жүйесін қаржыландыру стратегияларын оңтайландыру есептерінде шешімдерді қабылдауды қолдау жүйелері (ШҚҚЖ) үшін модельдерді одан әрі дамыту міндеті өзекті болып қала береді.

2.2 Хакердің қаржы ресурстары жөнінде толық ақпарат берілген жағдай үшін жоғары оқу орынының ақпараттық білім беру ортасының киберқорғау құралдарын қаржыландырудың рационалды стратегияларын таңдау моделі

Екі ойыншыға (ЖОО-ның қорғаушысы және хакерге) өз мақсаттарына жету үшін қаржы ресурстары қажет. Шабуылдаушы тарап, мысалы, бөгде коммерциялық бағдарламалық қамтамасыз етуді ЖОО АББО-ны бұзу үшін пайдалана алады немесе ЖОО АББО-ға қызмет көрсететін персоналды сатып ала алады.

Диссертацияда ұсынылып отырған модель бисызықты көпқадамды сапа ойынының шешіміне негізделген.

Берілгені: 1 ойыншы (U)– ЖОО АББО-ны қорғаушысы ; 2 ойыншы (V) – компьютер қаскүнемдері (хакер). 1 және 2 ойыншылары динамикалық жүйені басқарады. Жүйе ойыншылардың қаржы стратегияларын сипаттайтын тәуелді қозғалыстары және сәйкес траекториялары бар бисызықты дискретті теңдеулер жүйесімен берілген. ЖОО АББО-ның КҚ жүйесін және киберқорғау шекараларын еңсеру құралдарын (мысалы, вирустық бағдарламалар) қаржыландыруды болжайтын ойыншылардың стратегиялар жиынын табу қажет.

Зерттеу жұмыстарына [39,47] сәйкес екі терминалды беттері бар – M_0, N_0. ЖОО АББО-ны қорғаушының мақсаты динамикалық жүйені өзінің басқару стратегияларының көмегімен M_0 терминалдық бетке әкелу. ЖОО АББО-ға шабуыл жасаушылардың қаржы жағдайдайлары кез-келген мөлшерде болуы мүмкін деген болжам жасаймыз. Хакердің(лердің) мақсаты жоғары оқу орнының қорғаушысы қандай қаржыландыру жасаса да, бұзуға бөлінетін қаржы ресурстарын басқару стратегияларының көмегімен динамикалық жүйені терминалды бетке әкелу.

Ойынның мақсаты - нысандарға бірінші немесе екінші бетке әкелуге мүмкіндік беретін нысандардың бастапқы күйлердің және олардың стратегияларының жиынын табу керек [45,49]. Шешім шексіз көп қадамды ойындар үшін үстемдік әдістерді (методов доминирования) қолдану арқылы табылады [52].

ЖОО АББО қорғаушысына $\{1,...,T\}$ (T – натурал сан) берілген уақыт аралығына $de(0)$ - қаржы ресурстары, ал хакерге – $ha(0)$ қаржы ресурстары бөлінген деп қарастырамыз. Бұл параметрлер $t=0$ кезде ЖОО АББО қорғаушының және хакердің мақсаттарына жету үшін берілген қаржы ресурстарының болжамды шамасын анықтайды. Зерттеу жұмыстарына [39,48,54] сәйкес, екі ойынның- көп қадамды және бір қадамды шешімдерін салыстыру жағдайында, біз ЖОО АББО қорғаушысы және хакердің төмендегі қасиеттеріне байланысты олардың бастапқы күйлердің жиындары беттесетінін көреміз [53].

1-Қасиет: Т қадам жасай отырып мақсатына жететін ойыншының «қалау» жиыны, оның ішінде $1/T$ ықтималдықпен аралас стратегиялар класындағы екінші ойыншыға оңтайлы қарсы тұру кезінде оңтайлы аралас стратегияны қолданған жағдайда бір қадам жасай отырып мақсатына жететін қаржы ресурстарының бастапқы күйлердің жиынымен сәйкес келеді.

Бастапқы t уақытта ЖОО АББО қорғаушысы $de(t)$ шаманы $\alpha(t)$-коэффициентке (өзгеру, өсу қарқыны) көбейтеді және $u(t):(u(t)\in[0,1])$ - шамасын таңдайды. $\alpha(t)\cdot de(t)$ -көбейтінді t уақыттағы ЖОО АББО қорғаушысының қаржы ресурстарын анықтауға мүмкіндік береді.

Осыған ұқсас, бастапқы t уақытта хакер $ha(t)$ шаманы $\beta(t)$- коэффициентке (өзгеру, өсу қарқыны) көбейтеді және $v(t)$: $v(t)\,(v(t)\in[0,1])$ - шамасын таңдайды. $\beta(t)\cdot ha(t)$ -көбейтінді хакердің t уақытта ЖОО АББО-ны бұзуға бөлінген қаржы ресурстарын анықтауға мүмкіндік береді.

Келесі белгілеулерді енгіземіз:

r_1 – ЖОО АББО-ны қорғау үшін жұмсаған қаржы ресурстарын біршама мөлшерін, ал хакерге ЖОО АББО-ны бұзу үшін қанша қаржы ресурстары қажет екенін көрсететін коэффициент.

r_2 – Хакердің ЖОО АББО-ны бұзу үшін жұмсаған қаржы ресурстарының мөлшерін, ал қорғаушы үшін ЖОО АББО-ны қорғап қалуға қанша қаржы ресурстары қажет екенін көрсететін коэффициент.

Демек, зерттеу жұмыстарын [51-55] ескере отырып, жоғары оқу орнының АББО қорғаушының және шабуылдаушының қаржы ресурстарының өзгеру динамикасын төмендегідей дискретті теңдеулер жүйесі арқылы сипаттауға болады:

$$de(t+1)=\alpha(t)\cdot de(t)-u(t)\cdot\alpha(t)\cdot de(t)-r_2\cdot v(t)\cdot\beta(t)\cdot ha(t); \quad (2.1)$$

$$ha(t+1)=\beta(t)\cdot ha(t)-v(t)\cdot\beta(t)\cdot ha(t)-r_1\cdot u(t)\cdot\alpha(t)\cdot de(t). \quad (2.2)$$

t - уақытта шарттардың бірі орындалуы тиіс:

1) $de(t)\geq 0, ha(t)<0$. Егер шарт 1=*true болса*, онда ЖОО АББО-ның КҚ жүйесін қаржыландыру процедурасы аяқталады. Себебі, хакердің ЖОО АББО-ның қорғау жүйесін бұзу үшін қаржы ресурстары жетпей қалды;

2) $de(t)<0, ha(t)\geq 0$. Егер шарт 2=*true болса*, онда ЖОО АББО-ның КҚ жүйесін қаржыландыру процедурасы аяқталады. Себебі, ЖОО АББО-ys қорғаушының ЖОО ақпараттық - коммуникациялық жүйесін қорғау үшін қаржы ресурстары жетпей қалды.

3) $de(t)<0, ha(t)<0$. Егер шарт 3=*true болса*, онда ЖОО АББО-ның КҚ жүйесін қаржыландыру процедурасы аяқталады. Себебі, ЖОО АББО-ны қорғаушының да және хакердің де мақсаттарына жету үшін қаржы ресурстары жетпей қалды.

4) $de(t)\geq 0, ha(t)\geq 0$. Егер шарт 4=*true болса*, онда ЖОО АББО-ның КҚ жүйесін қаржыландыру процедурасы ары қарай жалғасады.

$de(t), ha(t)$-мәндері ЖОО АББО-ның КҚ жүйесіне бөлінген қаржы ресурстарының нәтижелерін бейнелейді.

Диссертацияда жоғары оқу орнының АББО-ның КҚ жүйесіне қаржы ресурстарын бөлу толық ақпараты бар позициялық көп қадамды ойын схемасының шеңберінде қарастырылды [39,46,52].

ЖОО АББО-ның КҚ жүйесіне қаржы ресурстарын бөлу процесін екі есеп түрінде қарастыруға болады:

1) Бірінші одақтас – ойыншы тұрғысынан есепті шешу;
2) Екінші одақтас – ойыншы тұрғысынан есепті шешу [46].
Есептер симметриялы болғандықтан, диссертация шеңберінде есепті бірінші одақтас – ойыншы тұрғысынан шешу қарастырылады.
$\{0,1,...,T\}$ жиынын T^* арқылы белгілейік.

Анықтама: Бірінші одақтас - ойыншының таза стратегиясы - бұл $(t,(de,ha))$ күйін $u(t,(de,ha)):0\le u(t,(de,ha))\le 1$ мәніне қоятын $u:T^*\cdot[0,1]\cdot[0,1]\to[0,1]$ функциясы.
Демек, бірінші одақтас - ойыншының таза стратегиясы t уақыт кезінде жағдайы туралы ақпаратқа $u(t,(de,ha))$ шамасын қоятын функция болады. Бұл шама t уақыт кезінде ЖОО АББО-да қорғаушы КҚ жүйесіне жұмсауды жоспарлаған қаржы ресурстардың бөлігін анықтайды.

Қарсылас - ойыншы (хакер) кез келген ақпарат (ойыншылардың жағдайы туралы, тіпті болашақта одақтас- ойыншының стратегиясын таңдау туралы және т.б. ақпараттар) негізінде ЖОО АББО-ны бұзуға бөлінетін қаржы ресурстарының мөлшерін және өзінің басқару әрекетін таңдай алады.
1 –ші есеп үшін стратегияларды анықтай отырып, ЖОО АББО-ның қорғаушысының W_1 -«қалау» жиынын анықтайық. Онда W_1 - төменде сипатталған қасиетке ие болатындай, ЖОО АББО қорғаушы және хакердің қаржы ресурстарының $(de(0),ha(0))$ - басапқы күйлердің жиындары [47].
2- Қасиет: W_1 бастапқы күйлер үшін қорғаушының стратегиясы бар болады, ол хакер өзінің стратегияларын қалай жүзеге асырса да, t уақытта $(de(0),ha(0))$-жүйенің жағдайын (1) шарт орындалатындай жағдайға "әкеледі". Бұл ретте хакерде t уақыттың алдыңғы кезеңдердің бірінде (t -дан қатаң кіші мәнедер үшін) (2) немесе (3) шарттарды орындауға "әкелетіндей" мүмкін стратегия болмайды.
2- қасиетке ие болатын ЖОО АББО-ны қорғаушының стратегиясын оңтайлы стратегия (қаржы ресурстарының шамасын анықтайтын стратегия) деп атаймыз.

1-ші есептің шешімі ЖОО АББО-ны қорғаушының «қалау» жиынын табудан тұрады. Сондай-ақ оның оңтайлы стратегиялары айқындалуы тиіс. Дәл осындай есеп хакер тұрғысынан қойылады.
1-ші есептің шешімі толық ақпаратпен берілген көпқадамды сапа ойындар теориясының әдістері арқылы табылады [48]. Бұл әдістер ойын параметрлерінің кез келген қатынасында шешім табуға мүмкіндік береді.
Диссертациялық жұмыстың осы бөлімінде мынадай шешім келтірілген: ойын параметрлерінің барлық қатынастарында «қалау» жиыны - W_1 және $u_*(.,.)$-оңтайлы стратегиялар.
а) жағдай $\alpha\le\beta$.

$$W_1^i = \left\{ \begin{matrix} (de(0), ha(0)) : k(i-1) \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot de(0) \prec k(i-2) \cdot \beta \cdot ha(0) \end{matrix} \right\}, i = 1,.. \qquad (2.3)$$

$$u_* = \{u_*(0,(de,ha)),...,u_*(i-1,(de,ha))\},$$

$$u_*(t,(de,ha)) = \{[1-(r_2 \cdot \beta \cdot ha)/(\alpha \cdot de)]\},$$

$(de,ha) \in R_+^2$ кезінде $\alpha \cdot de > r_2 \cdot \beta \cdot ha,$

кері жағдайда - анықталмаған;

мұндағы $t = 0,1,...,i-1.$

$r_1 \cdot r_2 = R_{1,2}, \frac{\alpha}{\beta} = \xi$ белгілейік.

Мұнда

$$k(i) = 1 + R_{1,2} - (r_1 \cdot \alpha \cdot \beta)/(\beta \cdot k(i-1));$$

$$k_{-1} = 0, k_0 = 1 + R_{1,2};$$

$$W_1 = \bigcup_{i=1}^{\infty} W_1^i.$$

$r_1 \cdot 2\alpha \cdot de(0) = \left\{ 1 + R_{1,2} + \left((1 + R_{1,2_2})^2 - 4 \cdot R_{1,2} \cdot \xi \right)^{0.5} \right] / 2 \cdot \beta \cdot ha(0) \}$- сәулесі тосқауыл болады [54].

Тосқауыл

$$(de(0), ha(0)) : r_1 \cdot \alpha \cdot de(0) \le \left\{ 1 + R_{1,2} + \left((1 + R_{1,2})^2 - 4 \cdot R_{1,2} \cdot \xi \right)^{0.5} \right] / 2 \cdot \beta \cdot ha(0) \}$$

-күйлерде қорғаушы қандай да бір уақытта мақсатына жете алмайтын жағдай.

ә) жағдай $\alpha \succ \beta,\ R_{1,2} \ge 1.$

Бұл жағдайда қорғаушының W_1- «қалау» жиыны саны шектеулі W_1^i жиындардың бірігуі. Дәлірек айтсақ $(N+2)$жиындардың бірігуі, мұндағы $N : k(i) \succ R_{1,2} \cdot \xi, i = 0,..., N-1; k(N) \le R_{1,2} \cdot \xi,$

$$W_1^i = \left\{ \begin{pmatrix} de(0), ha(0) : k(i-1) \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot de(0) \prec k(i-2) \cdot \beta \cdot ha(0) \end{pmatrix} \right\}, i = 1,..., N+1; \qquad (2.4)$$

$$W_1^{N+2} = \left\{ \begin{pmatrix} de(0), ha(0) : R_{1,2} \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot d(0) \prec k(N) \cdot \beta \cdot ha(0) \end{pmatrix} \right\}. \quad (2.5)$$

Онда ЖОО АББО-ның қорғаушысының оңтайлы қаржы стратегияларын $u_* = (u_*(0,(de,ha)),...,u_*(N+1,(de,ha))))$ былай анықтауға болады:

$u_*(0,(de,ha)) = \{0,\ (x,y) \in R_+^2$ *кезінде*, $\alpha \cdot de > r_2 \cdot \beta \cdot ha,$ және кері жағдайда - анықталмаған $\}$,

$u_*(t,(de,ha)) = \{[1-(r_2 \cdot \beta \cdot ha)/(\alpha \cdot de)],\ (de,ha) \in R_+^2$ *кезінде*, $\alpha \cdot de > r_2 \cdot \beta \cdot ha$ және кері жағдайда -анықталмаған; мұндағы $t = 1,..., N+1\}$.

б) жағдай $\alpha \succ \beta,\ R_{1,2} \prec 1.$

Бұл жағдайда да қорғаушының W_1- «қалау» жиыны саны шектеулі W_1^i жиындардың бірігуі. Дәлірек айтсақ $(N + i_* + 2)$ жиындардың бірігуі, мұндағы $N : k(i) \succ \xi, i = 0,..., N-1; k(N) \le \xi;$

i_* - $k(N) \cdot (\beta / \alpha)^{i_*+1} \prec R_{1,2}$ теңсіздікпен анықталатын, ең кіші бүтін оң сан.

Онда

$$W_1^i = \left\{ \begin{pmatrix} de(0), ha(0) : k(i-1) \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot de(0) \prec k(i-2) \cdot \beta \cdot ha(0) \end{pmatrix} \right\},\ i = 1,..., N+1. \quad (2.6)$$

Егер $i_* = 0,$ онда

$$W_1^i = \left\{ \begin{pmatrix} de(0), ha(0) : k(i-1) \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot de(0) \prec k(i-2) \cdot \beta \cdot ha(0) \end{pmatrix} \right\}, \quad (2.7)$$

$i = 1,..., N+1;$

$$W_1^{N+2} = \left\{ \begin{pmatrix} de(0), ha(0) : R_{1,2} \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot de(0) \prec k(N) \cdot \beta \cdot ha(0) \end{pmatrix} \right\}. \quad (2.8)$$

ЖОО АББО-ның қорғаушысының оңтайлы стратегиясын анықтау өрнегі б) жағдайға ұқсас.

Егер $i_* > 0,$ онда

$$W_1^{N+1+j} = \left\{ \left(\begin{array}{l} de(0), ha(0) : k(N) \cdot \left(\frac{\beta}{\alpha}\right)^j \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot de(0) \prec k(N) \cdot \left(\frac{\beta}{\alpha}\right)^{j-1} \cdot \beta \cdot ha(0) \end{array} \right) \right\}, \quad (2.9)$$

$i = 1,..., i_*;$

$$W_1^{N+1+i_*} = \left\{ \begin{array}{l} de(0), ha(0) : R_{1,2} \cdot \beta \cdot ha(0) \le \\ \le r_1 \cdot \alpha \cdot de(0) \prec k(N) \cdot \left(\frac{\beta}{\alpha}\right)^{i_*} \cdot \beta \cdot ha(0) \end{array} \right\}. \quad (2.10)$$

Онда, бұл жағдайда оңтайлы стратегияны $u_* = (u_*(0,(de,ha)),..., u_*(N+1+i_*,(de,ha)))$ былай анықтаймыз:

$u_*(i,(de,ha)) = \{0, \quad (de,ha) \in R_+^2$ *кезінде*, $\alpha \cdot de > r_2 \cdot \beta \cdot ha,$ және кері жағдайда - анықталмаған; $i = 0,..., i_*\},$

$u_*(i,(de,ha)) = \{[1-(r_2 \cdot \beta \cdot ha)/(\alpha \cdot de)],$

$(de,ha) \in R_+^2$ *кезінде*, $\alpha \cdot de > r_2 \cdot \beta \cdot ha, \quad i \ge i_* + 1$ және кері жағдайда - анықталмаған; $t = 1,..., N+1\}$

Бұған дейін ЖОО АББО қорғаушысының қаржы ресурстары шектеулі болады деп ескертілген. Қаржы ресурстарының (ҚР) максималды мәнін Ω арқылы белгілейік. Онда мұндай шектеу кезінде қорғаушының W_1^*-«қалау» жиыны W_1-жиын мен $\{(de(0), ha(0)) : (de(0), ha(0)) \in R_+^2, de(0) \le \Omega\}$- жиынның қиылысуын білдіретін болады.

Бұдан:

$$W_1^* = W_1 \cap \left\{ \begin{array}{l} (de(0), ha(0)) : (de(0), ha(0)) \in R_+^2, \\ de(0) \le \Omega \end{array} \right\}. \quad (2.11)$$

Осылайша, сияқты хакер үшін де «қалау» жиынын табуға болады. Бұл кезде де хакердің қаржы ресурстары шектеулі деп ойлаймыз. Осылайша, екінші одақтас (хакер) - ойыншы тұрғысынан 2- есепті шешуге болады. Бұл I ширекте $(de(0), ha(0))$- жазықтықта үш жиын түрінде көрсетуге мүмкіндік береді (ұшы $(0,0)$-нүкте болатын конустар). Бірінші жиын (конус) $0X$ осіне жақын жататын жиын ЖОО АББО қорғаушы үшін «қалау» жиыны болады. Екінші жиын (конус) хакер

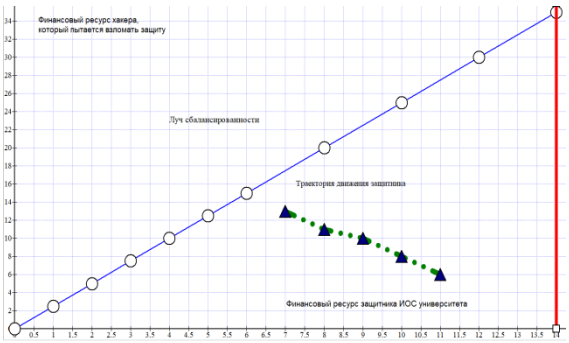
үшін «қалау» жиыны. Үшінші жиын (конус) екі ойыншының тарапынан да бейтарап жиын болады. Имитациялық эксперименттер PTC Mathcad 4 пакетінде орындалған. Имитациялық эксперименттердің нәтижелері 4- кестеде және суреттерде көрсетілген (суреттер 10,11,12). Имитациялық эксперименттің мақсаты: ойыншылар, атап айтқанда ЖОО АББО қорғаушысы және хакердің стратегиялар жиынын анықтау; ойыншылардың қаржы ресурстарын жоғалтуына байланысты тәуекелдерді модельдеу. Графиктердегі тепе –теңдесу сәулесі (ТТС) дөңгелек маркерлі тұтас сызықпен көрсетілген. Келесі аймақтар көрсетілген: ТТС астында – ЖОО АББО қорғаушының «қалау» аймағы; ТТС үстінде –хакердің «қалау» аймағы (сурет 10).

ЖОО АББО-ны қорғаушының қозғалыстар траекториясы үшбұрыш маркерлі нүкте сызықпен бейнеленген. Квадрат маркерлі тұтас сызықпен ЖОО АББО қорғаушысының қаржы ресурстарының шектеулері көрсетілген. Жүргізілген есептеулердің сайлылығын тексеру мақсатында модельдің көмегімен алынған нәтижелер Украинадағы «Украинаның биоресурстар және табиғатты пайдалану ұлттық университетінде» (Киев) және Қазақстандағы коммерциялық емес акционерлік қоғамы **«**Шәкәрім атындағы университетінде» (Семей) сынақтан өткізілді (Қосымша Б).

ЖОО АББО-ны қорғаушы ойыншы бастапқы қаржы ресурстарының көлемі бойынша артықшылықтарға ие болған жағдай қарастырылған (сурет 10). Себебі, бұл ресурстар ЖОО АББО-ны қорғаушының «қалау» жиынында орналасқан және ойын параметрлері арқылы есептелінеді. Қорғаушы өзінің оңтайлы стратегиясын қолдана отырып, өз мақсатына жетеді, өйткені бастапқы уақытта шектеулі болғанына қарамастан, қаржы ресурстары жеткілікті.

Кесте 4. ЖОО АББО қорғаушысының стратегиясын таңдау бойынша имитациялық эксперименттің нәтижелері

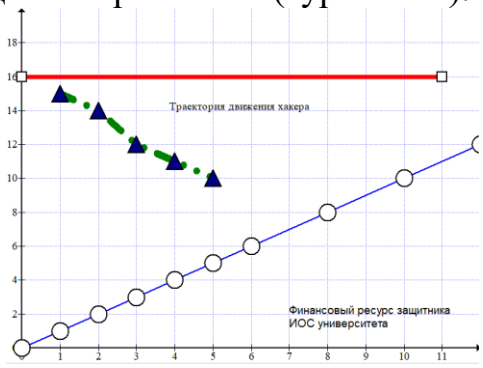
№ ИЭ	Модельдеу нәтижелері		
	Ойыншылардың ҚР-сы шектелмеген	Ойыншылардың ҚР-сына шектеу қойылған	
1	2	3	
1	(*de*(0), *ha*(0))=(10.0, 13.2); (*de*(1), *ha*(1))=(12.0, 11.36); (*de*(2), *ha*(2))=(14.0, 10.36); (*de*(3), *ha*(3))=(16.0, 8.4); (*de*(4), *ha*(4)) = (18.0, 6.4).	$\Omega = 14$ ЖОО АББО қорғ.ҚР-на қойылған шектеу	(*de*(0), *ha*(0)) = (7.0, 13.0); (*de*(1), *ha*(1))=(8.0, 11.0); (*de*(2), *ha*(2)) = (9.0, 10.0); (*de*(3), *ha*(3)) = (10.0, 8.0); (*de*(4), *ha*(4)) = (11.0, 6.0).
2	(*de*(0), *ha*(0))=(5.0, 10.0); (*de*(1), *ha*(1))=(4.0, 12.0); (*de*(2), *ha*(2))=(3.0, 13.0); (*de*(3), *ha*(3))=(2.0, 15.0); (*de*(4), *ha*(4))=(1.0, 17.0).	$\Omega = 16$ Хакердің ҚР-на қойылған шектеу	(*de*(0), *ha*(0))=(5.0, 10.0); (*de*(1), *ha*(1))=(4.0, 11.0); (*de*(2), *ha*(2))=(3.0, 12.0); (*de*(3), *ha*(3))=(2.0, 14.0); (*de*(4), *ha*(4))=(1.0, 15.0).
3	(*de*(0), *ha*(0))=(5.0, 20.0); (*de*(1), *ha*(1))=(4.0, 16.0); (*de*(2), *ha*(2))=(3.0, 12.0); (*de*(3), *ha*(3)) = (2.0, 8.0), (*de*(4); *ha*(4)) = (1.0, 4.0).	$\Omega = 7$ ЖОО АББО қорғаушы сының ҚР-на қойылған шектеу	(*de*(0), *ha*(0)) = (5.0, 15.0); (*de*(1), *ha*(1)) = (4.0, 12.0); (*de*(2), *ha*(2))=(3.0, 9.0), (*de*(3), *ha*(3))=(2.0, 6.0); (*de*(4), *ha*(4)) = (1.0, 3.0).



Сурет 10 – АББО-ны қорғаушы ойыншының рационалды траекториясы мен қолайлы аймақтары

ЖОО АББО-ны қорғаушының мақсаты- жүйенің жағдайын "өзінің" терминалды бетіне келтіру [55]. I ширекте жазықтықта (0,0) нүктеден шығатын сәулелердің жиынтығы қарастырылған. Бұл сәулелер мына қатынаспен анықталады: $ha = (2.5 - 1/n) \cdot de.$ Бұл сәулелер n қадамдағы бірінші ойыншының «қалау» жиынын береді. Мына қатынас арқылы берілген сәуле - $ha = (2.5) \cdot de$ тепе-теңдесу сәулесі болады.

ЖОО АББО-ны қорғаушының оңтайлы емес іс - әрекетін (оңтайлы стратегияларын іске асыруға сәйкес келмейтін әрекеттер) қолданғанын және ойыншылардың бастапқы жағдайы хакердің «қалау» аймағында орналасқанын пайдаланған хакердің жағдайы көрсетілген (суретте 11).



Сурет 11 – АББО қорғаушысын жеңуге тырысқан, хакер ойыншының рационалды траекториясы мен қолайлы аймақтары

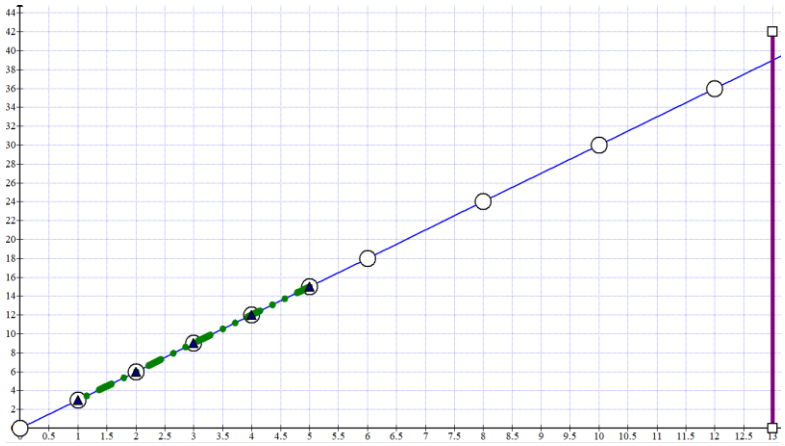
Хакерде қаржы ресурстар жеткілікті және бастапқы уақытта қаржы ресурстарының шектеулі болғанына қарамастан, ол жүйенің жағдайын "өзінің" терминалды бетіне "әкеледі".

I ширекте жазықтықта (0,0) нүктеден шығатын сәулелердің жиынтығы қарастырылған. Сәулелер мына қатынаспен анықталады: $h = (2 + 1/n) \cdot d.$ Сәулелер

n қадамдағы бірінші ойыншының «қалау» жиынын береді. Мына қатынас арқылы берілген сәуле - $h(0)=2\cdot d(0)$ тепе-теңдесу сәулесі болады. W_1^n жиындар келесі қасиеттерге ие ойыншылардың күйлерінің жиыны.

Қасиет: егер ойын W_1^n басталатын болса, онда қорғаушы өзінің мақсатына қорғаушы мен хакер өздерінің оңтайлы аралас стратегияларын қолданған кезде $(1/n)$ ықтималдықпен жетеді.

Жүйенің бастапқы жағдайы тепе -теңдесу сәулесінде жататын жағдай көрсетілген (сурет 12). Қорғаушы және хакер өздерінің оңтайлы стратегияларын пайдалана отырып, сәуле бойымен «қозғалады». Бұл бір уақытта қорғаушыны да, хакерді де «қанағаттандырады».



Сурет 12 – Имитациялық эксперименттің нәтижелері 3.
Жүйенің «тұрақтылығы»

Имитациялық экспериментті жүзеге асыру барысында біздің моделіміз, сондай-ақ диссертацияның 4-тарауында сипатталған оның бағдарламалық жүзеге асырылуы ЖОО АББО-ның КҚ жүйесін қаржыландыру саласында шешімдер қабылдауды тиімді қолдауды қамтамасыз етуге қабілетті екенін көрсетеміз.

Жұмыстың осы бөлімінде ұсынылған тәсіл ЖОО АББО-ның КҚ жүйесіне қаржы салымдарын моделдеу процесстерінде белгісіздікті (нақты ақпарат жоқ, сондықтан болжам жасау қиын жағдай) жоюға мүмкіндік берді. Бұл біздің зерттеуімізді басқа авторлардың жұмыстарынан ерекшелендіреді [54,55].

2.3 Хакердің қаржы ресурстары жөнінде толық ақпарат берілмеген жағдай үшін жоғары оқу орынының ақпараттық білім беру ортасын қорғаушының «қалау» жиынын және рационалды стратегияларын анықтайтын модель

Диссертациялық зерттеудің осы бөлімінде, оқу орынының, мысалы ірі оқу орынының КҚ және ақпаратты қорғау құралдарын қаржылындыру бойынша

рационалды стратегияларды таңдау есептерінде ШҚҚЖ құруға мүмкіндік беретін модельдер ұсынылған.

Ойындар теориясы шеңберінде екі тарап қарастырылады: №1 ойыншы – ЖОО АББО-ны қорғаушы; №2 ойыншы – компьютер қаскүнемдері. Екі ойыншы өз мақсаттарына жету үшін қаржы ресурстарын пайдаланады [50].

Ойыншыларда сәйкесінше $x(0)$ және $y(0)$ қаржы ресурстары бар. Өзара әрекеттесу уақыты берілген $\{0,1,...,T\}$, мұндағы Т – натурал сан. Ойыншылардың (ЖОО АББО-ны қорғаушы және компьютер қаскүнемдері) өзара әрекеттері бисызықты көпқадамды сапа ойынын білдіреді. Ойын барысында ойыншылар кезекпен ойнайды. Қорғаушы үшін компьютер қаскүнемдердің қаржы ресурстары туралы ақпарат толық берілмеген деп саналсын. ЖОО АББО-ның қорғаушысына компьютер қаскүнемдерінің бастапқы күйлерінің үлестіру функциясы - $F_0(\cdot)$ белгілі деп есептеледі.

Берілгені:

1. $t = 2n, x(t),\ x(t+1) - t,\ t+1$ уақыт кезіндегі ЖОО АББО-ны қорғаушы күйі;
2. $y_2^{\xi}(t), y_2^{\xi}(t+1) - t, t+1$- уақыт кезінде компьютер қаскүнемдерінің кездейсоқ күйі.

Демек, $t+1,\ t+2$ уақытта ойыншылардың жағдайы төмендегі теңдіктерден анықталады:

$$\begin{aligned} x(t+1) &= \alpha(t)\cdot x(t) - u(t)\cdot\alpha(t)\cdot x(t); \\ y^{\xi}(t+1) &= y^{\xi}(t) - s_1\cdot u(t)\cdot\alpha(t)\cdot x(t); \end{aligned} \tag{2.12}$$

$$\begin{aligned} y^{\xi}(t+2) &= \beta(t)\cdot y^{\xi}(t+1) - \nu(t)\cdot\beta(t)\cdot y^{\xi}(t+1); \\ x(t+2) &= x(t+1) - s_2(t)\cdot\nu(t)\cdot\beta(t)\cdot y^{\xi}(t+1); \end{aligned} \tag{2.13}$$

мұндағы $u(t), \nu(t): u(t)\in[0,1],\ \nu(t)\in[0,1];\ s_1 > 0,\ s_2 > 0.$

$t\in\{0,2,4,...,2\cdot n\}$ уақыт кезінде ЖОО АББО-ны қорғаушы ойыншы $x(t)$ шаманы $\alpha(t)$ коэффициентке (өзгеру қарқыны, өсу қарқыны) көбейтеді. Бұдан әрі, ЖОО АББО-ны қорғаушы t уақыт кезінде АББО-ны қорғауға бөлінетін ЖОО АББО-ны қорғаушының $\alpha(t)\cdot x(t)$ ресурсының үлесін анықтайтын $u(t)$ $(u(t)\in[0,1])$ шаманы таңдайды.

Ойыншылардың жағдайы $t+1$ уақытта кезінде (2.12) және (2.13) қатынасынан анықталады. Демек, компьютер қаскүнемдердің ЖОО АББО-ны бұзу үшін өзінің қаржы стратегияларын жүзеге асыру барысында оған $s_1\cdot u(t)\cdot\alpha(t)\cdot x(t)$- қаржы ресурсын бөлуге мәжбүр.

s_1- параметр (коэффициент) компьютер қаскүнемдері ЖОО АББО-ны бұзу құралдарын жасауға немесе сатып алуға инвестициялауының «тиімділігін» сипаттайды.

Егер мына шарт ақиқат болса:

$$P\left(y^{\xi}(t+1)<0\right)\geq p_o,\ (0\leq p_o\leq 1), \tag{2.14}$$

онда ЖОО АББО-ны қорғаушы ойыншы ЖОО АББО-ны p_0 - ықтималдықпен қорғауға кепілдік берді деп айтуға болады. Бұл кезде ЖОО АББО-ны қорғаушы өзінің қаржы ресурсын қолданды.

Осылайша, ЖОО АББО-ны қорғаушы тарапынан ЖОО АББО-ның АҚЖ-сын және КҚ-ны қаржыландыру процесі аяқталады. Егер (2.14) шарт орындалмаса, онда ЖОО АББО-ны қорғаушы АҚЖ-ны және КҚ-ны одан әрі қаржыландыруды жалғастырады.

Екінші ойыншы (компьютер қаскүнемдері) ЖОО АББО-ның қорғау шекарасын өтуге бағытталған өзінің қаржы стратегияларын жүзеге асыру барысында ЖОО АББО қорғаушысы сияқты әрекет етеді. Бұл жағдайда ойыншылардың жағдайы (2.13) қатынаспен анықталады.

Егер шарт ақиқат болса:

$$P\left(x(t+2)>0\right)<p_1,\ (0\leq p_1\leq 1), \tag{2.15}$$

бұл жағдайда, компьютер қаскүнемдері ЖОО АББО-ның киберқауіпсіздігіне шығын келтірді деп айтуға болады. Бұл ретте мұндай нәтиженің болу ықтималдығы $(1-p_1)$ тең. Осы кезеңде ЖОО АББО-ның АҚЖ мен КҚ-ны қаржыландыру процесі тоқтатылды.

Атап айтқанда, ЖОО АББО-ны қорғаушы не себепті жеңілгеніне талдау жасап, ЖОО АББО-ның АҚЖ-ны және КҚ-ны қаржыландырудың жаңа стратегиясын таңдау керек. ЖОО АББО-ны қорғаушы төменде тұжырымдалған қасиеттерге жауап беретін өзінің бастапқы күйлердің жиынын табуға мүдделі деп ойлаймыз.

Ойынның қасиеттері:

1) егер ойын бастапқы күйден басталса, онда ЖОО АББО қорғаушысы өзінің басқару әсерлері (стратегияларының көмегімен) - $u(0),...,u(t)(t=2n)$ есебінен ЖОО АББО-ның киберқорғауын p_0- ден артық ықтималдықпен қамтамасыз ете алады;

2) ЖОО АББО-ны қорғаушы таңдаған қаржы стратегияларын компьютер қаскүнемдердің зиян келтірмеуіне $(1-p_1)$артық ықтималдықпен ықпал етеді.

3) «Ойын қасиеттерінде» сипатталған мұндай күйлердің жиыны ЖОО АББО-ны қорғаушының «қалау» жиынын білдіреді.

Бұдан әрі келесі белгілеулерді енгіземіз:

Ф – бір өлшемді кездейсоқ шамаларды үлестіру функциялары;

$2n - T$ -ға жақын натурал жұп сан;

$T^* = \{0,2,...,2n\}$ – натурал жұп сандардың жиыны.

Жоғарыда баяндалғанның негізінде мынадай анықтама енгізіледі:

ЖОО АББО-ны қорғаушы ойыншының таза қаржы стратегиялары - $u(t,x,F) \in [0,1], (F \in \Phi)$ болатындай $u(.,.,.): T^* \times R_+ \times \Phi \to [0,1]$ функция.

Демек, ЖОО АББО-ны қорғаушының қаржы стратегиялары - бұл қолда бар мәліметтерді негізге ала отырып, ойыншыға ЖОО АББО-ның АҚЖ және КҚ жүйелеріне қаржы ресурстарын бөлуді есептеуге мүмкіндік беретін ереже.

№ 2 ойыншы (компьютер қаскүнемдері) ЖОО АББО-ны бұзу мақсатында кез-келген ақпаратқа негізделе отырып, өзінің қаржы стратегияларын - $\nu(.)$ таңдауға мүмкіндігі бар. Ойыншылардың мақсаттары әр түрлі және мақсаттарына жету үшін түрлі қаржы стратегияларын ұстанады.

Диссертацияда келтірілген ойын моделі ((2.12), (2.13) өрнектертер) тәуекел шарттарында шешім қабылдау есебі болады [56]. Сонымен қатар, біздің модель ойыншылардың кезектесіп жүретін бірнеше терминалды беттері бар бисызықты көп қадамды сапа ойыны болады [55-60]. ЖОО АББО-ны қорғаушының «қалау» жиынын және оңтайлы стратегияларын табу параметрлерге байланысты болады.

ЖОО АББО-ны қорғаушының «қалау» жиыны былай сипатталған:

$$c(0) = \inf\{c'\}, d(0) = \inf\{d'\}, \; F_0(c') \geq p_0, F_0(d') \geq p_1. \qquad (2.16)$$

ЖОО АББО-ны қорғаушының «қалау» жиыны және оның оңтайлы стратегиялары $T = 1,3,...$ үшін табылады.

«қалау» жиыны үшін белгілеулер енгізейік:

$V_1^T(p_0, p_1)$- ЖОО АББО-ны қорғаушының «қалау» аймағы, атап айтқанда ойыншылардың бастапқы жағдайының, оның ішінде ол T жүрісте ЖОО АББО үшін АҚЖ-ны және КҚ-ны қаржыландыру процедурасын табысты аяқтайды.

$T = 1$ болғанда

$$V_1^1(p_0) = \{x(0): s_1 \cdot \alpha \cdot x(0) \geq c(0)\}.$$

Сондықтан, ЖОО АББО-ны қорғаушының оңтайлы қаржы стратегияларын мына түрде жазуға болады:

$$u_*(1,x,c) = \begin{cases} 1, \; for \; s_1 \cdot \alpha \cdot x \geq c; \\ 0, \; otherwise. \end{cases} \qquad (2.17)$$

Зерттеу барысында ЖОО киберқауіпсіздік жүйесін және ақпаратты қорғау жүйесін инвестициялаудың рационалды қаржы стратегияларын таңдауды модельдейтін ойын параметрлерінің қатынастарының барлық нұсқалары қарастырылды.

Зерттеу [53-59] жұмыстарына сәйкес

$\left\{x(0): x(0) \in R_+, c(0) \in R_+ \; c(0) = \left(\alpha / (s_2 \cdot \beta)\right) x(0)\right\}$ - сәуле кедергі (барьер) болады деп есептейік.

Мұны осылай түсіндіруге болады. $x(0): c(0) > \left(\alpha / (s_2 \cdot \beta)\right) x(0)$ күйде, ЖОО АББО қорғаушысы $p \geq p_0$ ықтималдықпен мақсатқа жетуі мүмкін емес. Бұл сәулені ЖОО АББО-ны қорғау құралдарын қаржыландыру процедурасы үшін тепе - теңдесу стохастикалық сәулесі деп атауға болады.

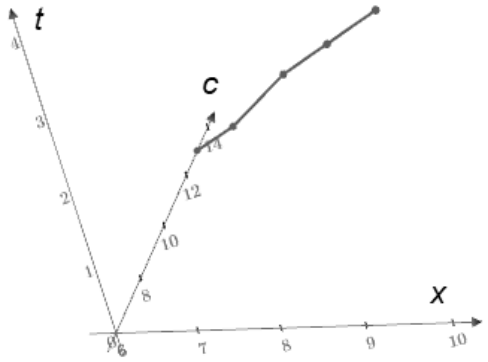
Моделді сынақтан өткізу мақсатында PTC MathCad 4.0. пакетінде есептеу эксперименттері орындалды.

Есептеу экспериментінің мақсаты:

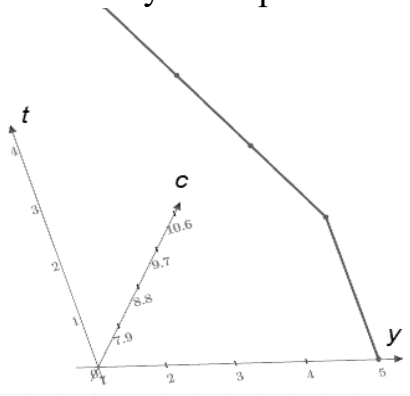
1) ойыншылардың (ЖОО АББО-ны қорғаушы және компьютер қаскүнемдері) қаржы стратегияларының жиынын анықтау;

2) ұсынылған математикалық модельдің сайлылығын бағалау.

Есептеу эксперименттерінің нәтижелері көрсетілген (суреттер 13,14).



Сурет 13 - № 1 есептеу экспериментінің нәтижелері



Сурет 14- № 2 есептеу экспериментінің нәтижелері

Диссертациялық жұмыстың осы бөлімінде ұсынылған шешім ойын параметрлерінің қатынастарының барлық жағдайлары үшін қарастырылды.

Есептеу экспериментінің нәтижелерін пайдалана отырып, ЖОО АББО-ны қорғаушының тиімді қаржы стратегияларын табамыз. Есептеу имитациялық эксперимент нәтижелерінің практикалық мәліметтерден максималды ауытқуы 7-12 % құрады.

Үш өлшемді I актантта $(t, x(0), c(0))$ (үш өлшемді кеңістікте) қарастырылады. t осі «нөлден, төменнен жоғары қарай жүреді» (суреттер 13,14). t уақыты- ЖОО АББО-ны қорғаушы және компьютер қаскүнемдері ойыншылардың қадамдарының саны. I актантта (0,0,0) нүктеден шығатын жазықтықтардың жиынтығы қарастырылды. Жазықтықтар $(0, x(0), c(0))$ жазықтыққа перпендикуляр және мына өрнекпен берілген: $c = \left(3.5 - \frac{1}{n}\right) \cdot x.$, n - кез келген оң сан.

Бұл жазықтықтар ЖОО АББО-ны қорғаушының «қалау» жиынын n қадамда беретіндей мүмкіндіктері бар. $p_0 = p_1$ деп алынды. Мысалы $V_1^n(p_0, p_0)$ жиыныны мынадай жиын:

Бұл жазықтықтар қорғаушының «қалау» жиынын n қадаммен орнатуға мүмкіндік береді

$$\left\{ \begin{array}{l} (n, x(0), c(0) : x(0), c(0)) \in R_+^2, \left(3.5 - 1/(n-1)\right) x(0) \le \\ \le c(0) < \left(3.5 - 1/(n)\right) x(0), t = n \end{array} \right\}. \qquad (2.18)$$

$n = 1$ болғанда

$$V_1^1(p_0) = \left\{ \begin{array}{l} (1, x(0), y(0) : x(0), c(0)) \in R_+^2, 0 \le \\ \le c(0) < (2.5) x(0), t = 1 \end{array} \right\}. \qquad (2.19)$$

$(x(0), c(0))$ - жазықтықтағы $c(0) = (3.5) \cdot x(0)$ - сәуле – стохастикалық тепе - теңдесу сәулесі (сурет 14) [60].

1-ші есептеу эксперименті ЖОО АББО-ны қорғаушы компьютер қаскүнемдеріне қарағанда қаржы ресурстары бойынша «артықшылығы» болған жағдайға сәйкес келеді (сурет 13). Бұл оған үш өлшемді кеңістікте (t, x, c) "жалпы" траекторияны басқаруға мүмкіндік береді. Сондай-ақ, ЖОО АББО-ны қорғаушы үшін қолайлы терминалды бетке өзінің қаржы ресурстарының траекториясын әкелу.

2-ші есептеу эксперименті сипатталған жағдай симметриялы (сурет 14). Атап айтқанда, екінші ойыншы (компьютер қаскүнемдері немесе хакер) қаржы ресурстары бойынша артықшылығы бар. Демек, компьютер қаскүнемдері өзінің қаржы ресурстарының траекториясын өзінің «қалау» жиынына әкелуге мүмкіндігі

бар. Осылайша, есептеу эксперименттерімен модельдің сайлылығы дәлелденді. Сондай-ақ модельдің ЖОО АББО-ның АҚЖ және КҚ жүйесін қаржыландыру саласында шешімдер қабылдауды нәтижелі қолдауды қамтамасыз ету мүмкіндігі расталды. Жұмыстың осы бөлімінде ұсынылған модель барлық бастапқы шарттар ескерілмеген шешім нұсқасының кемшіліктерін, атап айтқанда шабуылдаушы тараптың (компьютер қаскүнемдерінің - хакерлердің) қаржылай жағдайы туралы ақпарат толық берілмеген жағдайдағы кемшіліктерді жойды. Бұл тұрғыда жақсартылған модель бұрын берілген модельдерден [58,60], оның ішінде басқа авторлар ұсынған модельдерден ерекшеленеді [55,61].

Осылайша, осы саладағы алдыңғы зерттеулерге талдау жасай отырып, осы бөлімде бірінші рет оқу орынының, атап айтқанда ірі ЖОО-ның ақпараттық қауіпсіздік менеджментіне (басқаруына) ақпараттық - білім беру ортасының киберқауіпсіздігінің тиімді жүйелерін құрудың қаржы стратегияларын алдын ала бағалауды жүргізуге мүмкіндік беретін шешім ұсынылды. Модельдің айрықша ерекшелігі қорғау тарапы шабуылдаушы тараптың қаржы стратегиялары және оқу орнының ақпараттық-коммуникациялық жүйелерінің киберқауіпсіздік шекарасынан өтуге бағытталған оның қаржы ресурстарының жағдайы туралы толық ақпараты болмаған жағдай қарастырады. Модельдің сайлылығын тексеру үшін көп нұсқалы есептеу эксперименті қолданылған.

Ұсынылған модель жоғары оқу орындарының ақпараттық-коммуникациялық жүйелерінің ақпаратты қорғау жүйелеріне және киберқауіпсіздік жүйелеріне инвестициялаудың рационалды қаржы стратегияларын таңдау бойынша шешімдер қабылдауды қолдау интеллектуалданған жүйеге арналған. Модельде ақпараты толық берілмеген есепті шешу үшін динамикалық бағдарламалау әдісі қолданылады.

Екінші тарау бойынша қорытындылар

Диссертациялық жұмыстың екінші бөлімінде келесі нәтижелер алынды:

– ЖОО АББО-ның ақпаратты қорғау жүйесін және киберқауіпсіздік жүйесін инвестициялаудың рационалды қаржы стратегияларын таңдау бойынша шешімдер қабылдауды қолдау интеллектуализацияланған жүйесі үшін модель ұсынылды. Модельде ақпараты толық берілмеген есепті шешу үшін динамикалық бағдарламалау әдісі қолданылады. Бұл қолданыстағы шешімдерге қарағанда, ЖОО АББО-ны қорғаушы тарапына ақпараттық жүйелерді қорғау кезінде ресурсттардың шығындарын талап ететін жағдайлардың нұсқалары үшін шешімдерді неғұрлым тиімді табуға мүмкіндік берді;

– ақпараттық мазмұн қорғаныс жағынан ойыншылардың ресурстарын қажет ететін есептеу эксперименттерінің нәтижелері сипатталған. Ойынның шешімі ЖОО АББО-ны қорғаушы және ЖОО АББО - ның киберқауіпсіздік шекарасын өтуге ұмтылатын компьютер қаскүнемдері жағынан ойыншылардың ойын параметрлер қатынасының барлық жағдайлары үшін келтірілген. ЖОО АББО-ны

қорғаушының оңтайлы әрекеттерінің (қаржы стратегияларының) нұсқалары табылды;

– ЖОО АББО-ны қорғаушы тарапына хакердің қаржы ресурстарының жағдайы бойынша мәліметтер толық берілмеген жағдайлар қарастырылды.

Есептеу эксперименттері барысында ұсынылған математикалық модельдердің сайлылығы дәлелденді. Есептеу эксперименттері нәтижелерінің практикалық мәліметтерден (қолданыстағы мәліметтерден) ауытқуы 12% - дан аспайды.

3 ПЕТРИ ЖЕЛІЛЕРІНІҢ АППАРАТЫН ПАЙДАЛАНА ОТЫРЫП ЖОҒАРЫ ОҚУ ОРНЫНЫҢ АҚПАРАТТЫҚ БІЛІМ БЕРУ ОРТАСЫНДА ҚОЛЖЕТІМДІЛІК ҚҰҚЫҚТАРЫН БЕЙІМДЕЛГЕН БАСҚАРУДЫҢ ТҰЖЫРЫМДАМАЛЫҚ МОДЕЛІ

Білім беруде ақпараттық технологияларды (АТ) және ақпараттық технологиялар жүйелерін (АТЖ) қолданудың заманауй деңгейі өте жоғары. Диссертациялық жұмыстың 1 тарауында көрсетілгендей, жоғары оқу орнының ақпараттық білім беру ортасы (ЖОО АББО) деген жаңа термин пайда болды [3-7]. ЖОО АББО-ны ақпараттандырудың кез келген нысаны сияқты ақпаратты қорғау және киберқауіпсіздік бойынша міндеттерді шешуді талап етеді [2-19]. Бұл ретте АТ саласындағы мамандардың көпшілігі ақпараттың функционалдық мақсатына қарамастан тұтастығын, құпиялылығын және қолжетімділікті сақтау қажеттілігі бірінші кезекте екенін атап өтеді [10-18].

ЖОО АББО-ны қорғаудың және КҚ-ның тиімді жүйесін құрудағы жалпы бастапқы міндет нақты қорғау нысанын зерттеу, потенциалды бұзушының (компьютер қаскүнемдері) және киберқатер модельдерін қалыптастыру. Жоғарыда көрсетілген қадамдарды жүзеге асырудың нәтижесі ЖОО АББО-ны ақпаратты қорғау жүйелеріне (АҚЖ) қойылатын сай талаптар алуға мүмкіндік береді.

Кибершабуылдардың күрделенуі жағдайында ақпараттық қауіпсіздік (АҚ) қызметінің талдаушыларына кибершабуылдарға, аномалияларға (нормадан ауытқуларға) және қатерлерге жедел әрекет ету қажет. Компьютер қаскүнемдері -нің тарапынан деструктивті араласуына немесе ақпараттандыру нысандарының, оның ішінде ЖОО АББО-ның жұмысына жауапсыз персонал тарапына қарсы әрекет ету тапсырмаларында шешімдерді қабылдаудың нәтижелілігін арттырудың жаңа тәсілдерін іздеу есебі өзекті.

Көптеген мамандардың пікірінше, Петри желісі теориясында ЖОО АББО-ны қорғаудың түрлі жүйелерінің функционалдық модельдерін сипаттау мүмкіндігі жеткілікті перспективалы болады [86-89]. Мұндай көрініс ақпаратты қорғау және КҚ талдаушыларына ЖОО АББО-дағы киберқауіптерді нақтылауға мүмкіндік береді. Сонымен қатар, жаңа киберқауіптер болар алдында ЖОО АББО-ның осалдығын потенциалды анықтайтын күйлерді табуы мүмкін. Сонымен қатар, Петри (және Петри–Марков) желілері мен Петридің боялған желілеріне негізделген осы модельді ЖОО АББО үшін киберқатерді талдау процесінде жобаланған шешімдерді қабылдауды қолдау интеллектуалды жүйелеріне математикалық және алгоритмдік құраушы ретінде қолдану перспективасы қарастырылады. Біздің ойымызша, осы пікірлер жұмысымызды өзекті етеді және ЖОО АББО-ның ақпаратты қорғау және КҚ міндеттерінде шешімдерді қабылдауды қолдау интеллектуалды жүйесін (ШҚҚИЖ) құру жұмыстары барысында нәтижелілікті арттырады.

[64-71] жұмыстарда киберқатерлердің моделін сипаттау үшін Петри желілерін қолдануға арналған зерттеу нәтижелері ұсынылған. Бұл жұмыстар осы міндетте айтарлықтай теориялық үлес қосса да, біздің ойымызша, авторлар ұсынған модельдерді ЖОО АББО-ның ақпаратты қорғау және КҚ бойынша құрылған ШҚҚИЖ-де бағдарламалық жүзеге асыру (программалау) біршама қиынға соғады.

Зерттеу жұмыстарын [63,67], [73] негізге ала отырып, ЖОО АББО-ның қорғалуын бағалау міндетін өзектендіру кезінде жеткілікті түрде көрнекі көрсетілген қатерлер кестесін қолдана отырып, қатерлердің модельдерін құруға болады. Бірақ, бұрын көрсетілгендей, бұл тәсілмен қатерлердің моделін құру көп еңбекті қажет етеді. Сонымен қатар, қатерлер санының өсуі мұндай кестелік форматты толтыру және онымен жұмыс істеу кезінде, әсіресе КҚ саласында жұмыс тәжірибесі аз мамандарға қиындықтар туғызады.

Петри (және Петри–Марков) желілері шабуылдаушы (компьютер қаскүнемдері) модельдерін сипаттау үшін де сәтті қолданылды. Алайда, авторлар ЖОО АББО-ға шабуылдаушы (компьютер қаскүнемдері) моделін, атап айтқанда оны графтар теориясы негізіндегі модельдермен біріктіру арқылы нақтылау мүмкіндігін қарастырмаған, бұл ЖОО АББО-ның киберқорғау периметрлерінен (шекарасынан) ҚҚас-тың ықтимал өту процесіндегі күйлердің ауысуын неғұрлым дәл сипаттауға мүмкіндік берер еді. ЖОО АББО-ның киберқорғау периметрлерін (шекарасынан) ҚҚас-тың ықтимал еңсеру процесіндегі күйлердің ауысуын сипаттауға мүмкіндік берер еді.

Зерттеу жұмыстарында [65] АҚЖ-ның модельдері Петри желісінде алдын ала анықталған, кибершабуыл болуы мүмкін қарапайым операциялардың тізбегі ретінде қарастырылды. Модельдер берілген уақыт аралығында түрлі шабуылдарды жүзеге асыру ықтималдығын есептеуге мүмкіндік береді. Алайда, [66-75] зерттеулерде қарастырылған модельдер жаңа киберқатерлердің жұмыс істеу процесінде уақытқа байланысты сипаттамаларды есептеуге мүмкіндік бермеді.

Мына [65-68] зерттеу жұмыстарында Петри желілерінде негізделген және ақпараттық жүйелерде (АЖ) қатерлерді жүзеге асыру процестерін сипаттайтын модельдер ұсынылды. Бұл модельдер нысандардың қорғалуының көптеген параметрлерін, атап айтқанда, қатерді жүзеге асыру ықтималдығын, қатерлерді жүзеге асыруға кеткен уақытты бағалауды жүргізуге мүмкіндіктері болғанына қарамастан, киберқаскүнемдердің өзара келісу әрекеттері соңына дейін аяқталмаған болып көрінеді. Атап айтқанда, бұл жұмыстарда әртүрлі кластарға жататын шабуылдар барысында АЖ күйінің өзгеруі кезінде туындайтын даулы жағдайларды шешу міндеті зерттелмеген. Бұл жағдай, біздің ойымызша, осы зерттеулердің практикада қолданылуын шектейді.

Петри желілері (ПЖ) әртүрлі ақпараттандыру объектілерінің қорғалу күйлерін модельдеуге байланысты процестерді модельдеу үшін жеткілікті ыңғайлы құрал болып табылады. ПЖ- классикалық формализмнің көптеген

түрлерін, модификациялары мен жалпылауын қамтитын математикалық модельдер кластарының иерархиясы. ПЖ-ның және ақпаратты қорғау, КҚ-ны қамтамасыз ету процестерін сипаттайтын модельдердің негізгі артықшылықтары күрделі динамикалық дискретті жүйелердің құрылымын адекватты түрде көрсету мүмкіндігі болып табылады. Сондай-ақ, «шарт-күй» терминдерін қолдана отырып, модельденген жүйелердің өнімділігін, олардың құрылымының оңтайлылығын, олардың жұмыс істеу процесінің тиімділігін, белгілі бір күйлерге жету мүмкіндігін және т. б. қолдана отырып АҚЖ-ның жұмыс істеу процестерінің логикалық - уақыттық ерекшеліктерін модельдеу үшін ПЖ-ны қолдануға болады. ПЖ иерархиялық құрылымының мүмкіндіктері күрделі жүйелер мен процестердің, соның ішінде АҚЖ мен КҚ үшін бөлінуін қамтамасыз ете отырып, әр түрлі дәрежедегі модельдерді нақтылауға мүмкіндік береді. ПЖ аппараты іс жүзінде баламасыз болып табылады, егер басқару объектісі, мысалы, ЖОО АББО желісі және оның жекелеген бөліктері (ішкі жиындары) синхронды емес жұмыс істейтін болса. ПЖ-ны графикалық түрде ұсынуға болады, бұл олардың көрнекілігін көрсетеді және ПЖ-ны аналитикалық түрде де ұсынуға болады.

Осылайша, жаңа модельдерді біріктіру, сондай-ақ, Петри желілері аппаратының мүмкіндіктерін пайдалана отырып және Петри желілерінің визуализациялау потенциалын ескере отырып, ЖОО АББО-ның киберқорғауын бейімделген басқарудың қолданыстағы модельдері мен әдістерін толықтыру, ЖОО АББО мен басқа да ірі жоғары оқу орындары үшін қорғалу жағдайын болжау үшін тиімді құрал болуы мүмкін. Бұл жаңа киберқатерлер үшін түсініктерді айтарлықтай жеңілдетуге мүмкіндік береді және әрі қарай әр түрлі ақпараттандыру нысандарының ақпаратты қорғау, АҚ және КҚ қызметтерінің талдаушылары осы ұсынылған тәсілдерді нәтижелі қолдануы мүмкін.

Сонымен, диссертациялық жұмыстың 3 тарауында мынадай есептерді шешу қажет:

– Петри желілерінің аппаратын қолдану арқылы ЖОО-ның киберқорғауын бейімделген басқарудың тұжырымдамалық моделін құру;

– жоғары оқу орындарының компьютер желілерінде қолданушылардың есептерін үлестіру (міндеттерін бөлу) модельдерін дамыту;

– ЖОО АББО -ның қауіпсіздік саясатының міндеттерімен мен талаптарынан және қолжетімділікке рұқсат етілген төбелердің сәйкестік дәрежесі сұранысынан қолжетімділік құқықтарын салыстыру міндетінде қолжетімділік құқықтарын бақылау әдісіне толықтырулар енгізу.

3.1 Жоғары оқу орынының ақпараттық білім беру ортасына қолжетімділік құқығын бейімделген басқарудың тұжырымдамалық моделі

Петри желілерінің аппаратын пайдалана отырып, қолданушылардың қолжетімділік құқықтарын бейімделген басқару есебін шешудің нақты мысалын және осы есепке сәйкес келетін бағдарламалық жабдығын қарастырайық. Бұл

бағдарламалық жабдық ЖОО АББО-ны қолданушыларының профилін нақтылауды автоматтандыруға және ЖОО АББО-дағы киберқатерді шешімдерді қабылдауды қолдау интеллектуалды жүйесі (ШҚҚИЖ) модулін интеграциялау арқылы бейтараптандыру тәсілдерін ұсынуға мүмкіндік береді

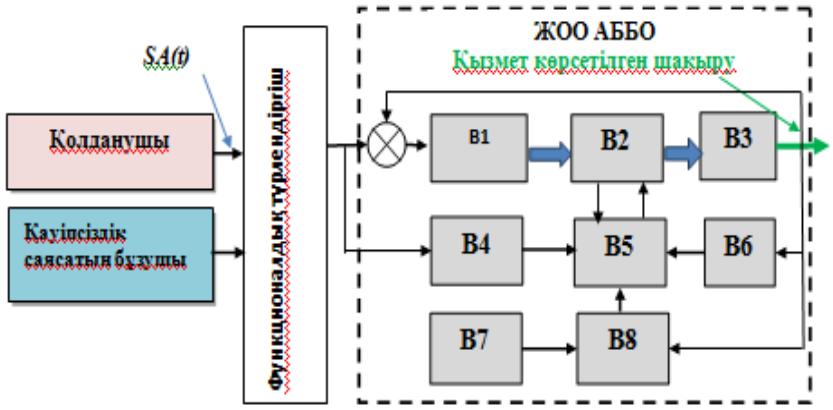
Қолжетімділік құқықтарын басқару есептерінің қойылымын осылай тұжырымдаймыз:

1) берілген ЖОО АББО үшін қолжетімділікті шектеу моделін құру;
2) модельдің басқарылмалы параметрлерін анықтау;
3) ЖОО АББО үшін ақпараттың құпиялылығын бұзу тәуекелділігін параметрлер арқылы сипаттау.

ЖОО АББО-дағы қолжетімділікті шектеу схемасын оңтайландыру бойынша есептің формальды математикалық қойылымы (сурет 15).

Бастапқы мәліметтер:

1) ЖОО АББО-ның қолжетімді нысандары– $AO = \{ao_i\}, i = \overline{1, I}$;
2) ЖОО АББО-ның қолжетімді субъектілері– $SA = \{sa_j\}, j = \overline{1, J}$;
3) ЖОО АББО -ның коммуникациялық төбелері (КТ) – $CN = \{cn_k\}, k = \overline{1, K}$;
4) ЖОО АББО-ның қолжетімділік қауіпсіздігі метрикасының мәнін берілген деңгейде қолдап отыруға мүмкіндік беретін бейімделген механизм– $AM^0 = \{am^0_{i,j}\}, i = \overline{1, I}, \ j = \overline{1, J}$.



Сурет 15- ЖОО АББО-ның киберқорғауды бейімделген басқарудың тұжырымдамалық моделінің сызбасы

Суретте қабылданған белгілеулер: B1 – ЖОО АББО -ның ақпараттық өлшеу құрылғылар блогы; B2 – көп арналы басқару құрылғыларының блогы; B3 – ЖОО АББО -ның ресурстарға қолжетімділікті басқару нысаны ретінде; B4 – ЖОО АББО-ның күйлерді болжау блогы; B5 – қолжетімділік құқығы туралы шешімдерді қабылдау блогы; B6 – ЖОО АББО-ның қолжетімділіктің бұзылуына байланысты жүзеге асырылған қатерлер санын тиімді есептеу блогы; B7 – априорлық ақпарат блогы; B8 –модельдердің айнымалылар блогы.

Егер 5-кестеде сипатталған шарттар орындалса, ЖОО АББО-ны қорғаудың оңтайлы деңгейіне қол жеткізілді деп ойлаймыз.

Кесте 5 - ЖОО АББО–ны қорғаудың оңтайлы деңгейіне қол жеткізетін шарттар (ЖОО АББО-дағы қолжетімділікті басқаруды оңтайландыру тапсырмасы үшін)

No	Параметрлер	Шарттар
1	ЖОО АББО-ның қолжетімділік қауіпсіздігі метрикасының мәнін берілген деңгейде қолдап отыруға мүмкіндік беретін бейімделген механизм.	$am_{i,j} = \begin{cases} 1, \text{ if } am_i \text{ it is placed on} \\ \text{a node } cm_k; \\ 0, \text{ Otherwise}. \end{cases}$
2	Ресурстарға ықтимал рұқсат етілмеген қолжетімділіктен болатын шығын – $DA^0 = \{da^0_{i,j}\}, i = \overline{1,I},\ j = \overline{1,J}$	Ескертуді қараңыз.
3	ЖОО АББО-ның есептеу желісінің құрылымы – $NS = \{ns_{m,n}\}, m,n = \overline{1,K}$	$ns_{m,n} = \begin{cases} 1, \text{ if } (cn_m \in NS_o)\,\& \\ (cn_n \in NS_o); \\ 0, \text{ Otherwise}. \end{cases}$ *where* NS_o – Network objects.
Басқарылатын параметрлер (ақпаратты қорғаужәне КҚ администраторы береді)		
1	ЖОО АББО-ның ресурстарына жалпы қолжетімділік белгілері – $SV = \{sv_i\}$	$sv_i = \begin{cases} 1, \text{ if the general access} \\ \text{to a node } sv_i \\ \text{is allowed}; \\ 0, \text{ Otherwise}. \end{cases}$
2	ЖОО АББО-ның төбелеріне AO (қолжетімді нысандарын немесе құрылғыларды) орналастыру – $MP^1 = [mp^1_{i,k}]$	$mp^1_{i,k} = \begin{cases} 1, \text{ if } ao_i \in cn_k; \\ 0, \text{ Otherwise}. \end{cases}$
3	ЖОО АББО-ның төбелеріне SA орналастыру – $MP^2 = [mp^2_{j,k}]$.	$mp^2_{j,k} = \begin{cases} 1, \text{ if } sa_j \in cn_k; \\ 0, \text{ Otherwise}. \end{cases}$
Ескерту**:** Ресурстарға ықтимал рұқсат етілмеген қолжетімділік болған кездегі шығынды (кестедегі 2 жол) ЖОО АББО-ның төбелерінде ақпараттық ресурстарды қорғау шаралары арқылы, сондай-ақ қолданушының профилі арқылы анықтаймыз (ықтимал бұзушылардың сипаттамаларын ескере отырып, 6-кестені қараңыз).		

ЖОО АББО-ны қорғаудың оңтайлы деңгейіне қол жеткізетін шарттары (ЖОО АББО-ның қолжетімділікті басқаруды оңтайландыру тапсырмасы үшін) бұдан әрі 6-кестенің мәліметтерімен біріктіріп қарастырылады.

Кесте 6 - Ықтимал бұзушылардың сипаттамалары

Топтастыру	Сипаттамасы
Бұзушылық себептері бойынша	Пайдакүнемдік немесе басқа мақсатпен тұтастықты, құпиялықты, қолжетімділікті бұзу.
компьютер қаскүнемдері - нің ақпараттану деңгейі және біліктілік деңгейі бойынша	Бұзушы (немесе компьютер қаскүнемдері): 1) білім деңгейі жоғары; 2) ақпаратты жинау үшін білім деңгейі жеткілікті, танымал эксплойттарды қолданады және кибершабуылдарды жүзеге асыру үшін өзі бағдарламалық жабдықты жаза алады; 3) компьютер қаскүнемдері ЖОО АББО-да авторизацияланған қолданушы болып табылмайды.
Әрекет ету орны бойынша	ЖОО АББО-ның аймағына тікелей (физикалық) кірмейтін жағдай. Бұзушы қашықтан, мысалы, ортақ пайдалану желілері арқылы әрекет етеді.

ЖОО АББО-ның ақпараттық ресурстарына (ЖОО АББО АР) рұқсат етілмеген қолжетімділік нәтижесінде мақсатты функция ЖОО-да келтірілген ықтимал болатын қаржылай немесе өзге де шығындардың шамасы болады деп ойлаймыз. Бұл параметрді диссертация шеңберінде ЖОО-да нақты АББО үшін ақпараттық ресурстарға қолданушылардың қолжетімділікті нақты шектеуі мен қолжетімділікті рационалды шектеуінің арасындағы айырмашылықтың өлшемі ретінде анықтаймыз.

$$TF = \sum_{i=1}^{I}\sum_{j=1}^{J} da_{i,j}^{0} \cdot \left| am_{i,j} - am_{i,j}^{0} \right|, \qquad (3.1)$$

мұндағы $\{am_{i,j}\}$ – жүзеге асырылған қолжетімділік құқықтарын көрсететін жиын элементтері.

Айталық,

$$am_{i,j} = \sum_{k=1}^{K} ns_{i,k} \cdot w_{k,j}^{0}; \qquad (3.2)$$

$$w_{k,j}^{0} = w_{k,j}^{1} + sv_{i} \cdot \left(1 - w_{k,j}^{1}\right), \qquad (3.3)$$

$$w_{k,j}^{1} = \sum_{k=1}^{K} \left(mp_{i,k}^{2} \cdot mp_{k,j}^{1} \right). \qquad (3.4)$$

Осылайша, қолжетімділік құқықтарын шектеу есептерінің тұжырымдамасы алынды. Бұл есеп сызықты емес программалау есептеріне жатады. Есепті шешу

кезінде буль айнымалылары бойынша операциялар форматында басқарылмалы параметрлердің векторын қарастырамыз:

$$UD = \min \sum_{i=1}^{I} \sum_{j=1}^{J} da_{i,j}^{0} \cdot \left| am_{i,j} - am_{i,j}^{0} \right| \qquad (3.5)$$

келесі шектеулер үшін

$$\sum_{k-1}^{K} da_{i,j}^{1} \le 1 \qquad (3.6)$$

және

$$\sum_{k-1}^{K} da_{i,j}^{2} \le 1. \qquad (3.7)$$

Белсенді қолданушылардың профиліне нақтылауды жиі енгізу арнайы итерациялық алгоритмді қолдануды болжайды [77-80]. Бұл алгоритм сервердің нақты ЖОО АББО ресурстарын қолданушымен анық емес кері байланысына негізделген. Негізгі фактор - сұраныс статистикасы. Қарастырып отырған қолданушының ағымдағы профилін бағалау ЖОО АББО-ның ақпараттық ресурстары үшін қауіптілік дәрежесі бойынша қолданушыларды топтарға бөлу үшін қолданылды.

Қабылданды:

а) қолданушы;

ә) потенциалды қауіпті қоданушы;

б) қауіпті қоданушы;

в) бұзушы.

Қолжетімділікті басқару процедураларының баптауларын оңтайландыру осындай параметрлерді анықтау негізінде жүзеге асырылады:

1) Өту қарқындылығы $\lambda_{i,j}(t)$ (регрессиялық модельдер негізінде анықталды) [68,74];

2) ақпараттық қауіпсіздік саясатын бұзумен байланысты тәуекелдік параметр арқылы сипаттау кезінде ЖОО АББО-дағы ақпараттың барлық қасиеттері (құпиялылығы, тұтастығы және қолжетімділік) қарастырылды.

2-ші ретті келесі регрессиялық модель алынды [24]:

$$P_r(\tau) = da_0 + \sum_{k=1}^{m} da_k \cdot h_k + \sum_{ao=1}^{m} da_{ao,ao} \cdot h_{ao}^2 + \sum_{i,j=1}^{m} da_{i,j} \cdot h_i \cdot h_j, \; i \ne j,$$

Мұндағы $h = (h_1, ..., h_m)^T -$ нақты ЖОО АББО-ның желілерінде қолжетімділікті шектейтін ережелерді реттейтін басқарылмалы параметрлер, $\tau -$ уақыт.

Ресурстарға қолжетімділіктің үлестірілген схемасы бар кез- келген ЖОО АББО-ға қатысты абоненттік тапсырмалар моделі осылай анықталған:

$$\sum = (PN, PIS, AT, s_0, FTR, MRT, RES), \quad (3.8)$$

мұндағы $PN = (TGR, T, MPN, F)$ – ЖОО АББО АР (Петри желісімен ұсынылған);

$TGR = \{tgr\}$ – граф төбелерінің жиыны (төбелері - ЖОО АББО АР-ны жеткізуші);

$T = \{t\}$ – төбеден-төбеге ауысу саны;

$MPN = (mpn_1, ..., mpn_n)$ – Петри желісінің позицияларының белгілер саны;

F – көрші төбелердің арасындағы қарым-қатынас;

PIS – ақпараттық қауіпсіздік саясаты;

AT – ЖОО АББО АР қолданушылары бастамашылық жасаған, белсенді есептер;

s_0 – $S = \{s\}$ бастапқы күйі;

$FTR: PN \times AT \times MRT \times PIS \times A \to S$ – ЖОО АББО АР күйлерінің арасындағы ауысу функциясы;

$MRT = \langle CL, U \rangle$ – Петри желісіндегі маркерлер (белгілері бар позициялар саны);

CL – абоненттер (қолданушылар) (U) сұраныс салатын ресурстар классы;

RES – ЖОО АББО АР-ға қолжетімділік құқына сәйкес келетін ағымдағы позиция.

Алдыңғы есептеулерді ескере отырып, абоненттің (АР-ны қолданушы) қолжетімділік мүмкіндігі туралы шешім қабылдау үшін жұмыс істейтін "Қатер талдағыш» ([78] жұмысында толық сипатталған) бағдарламалық жабдығы үшін осындай ереже алынды:

егер екі жақты келісілген аутентификациялау процедурасы дұрыс өтсе, U абонентіне (ЖОО АББО АР қолданушысына) OWR иесінің меншігіндегі АР-ға қолжетімділікке рұқсат берілген.

АР OWR иесі үшін жергілікті есептік жазба анықталады. Бұл жазбада қауіпсіздік саясатына сәйкес барлық абоненттер және олардың қолжетімділіктерінің түрлері көрсетілген:

$$Has\ COMP\ Ass\ Ri(U, OWR, PIS) = \begin{pmatrix} Is\ TRU\ By\ U(U, OWR) \wedge \\ Is\ TRU\ By\ TGR(OWR, U) \wedge \\ \wedge (MapU\ To\ UD(OWR, U) \neq 0) \end{pmatrix} \wedge \quad (3.9)$$

$$Is\ Acc\ AL\ By\ PIS(U, OWR, PIS),$$

ЖОО АББО АР-ға қатысты абоненттер көрсетілген төбелердегі жергілікті есептік жазбалар Ob нысаны бойынша RI-қолжетімділік құқығына ие болуы міндетті:

$$Has\ FC\ Ass\ Ri\left(U,OWR,PIS,Ob,RI\right)=\begin{pmatrix} Is\ TRU\ \ By\ U\left(U,OWR\right)\wedge \\ \wedge\ Is\ TRU \\ By\ TGR\left(OWR,U\right)\wedge \\ \begin{pmatrix} ListU= \\ MapU\ To\ UD\left(OWR,U\right)\neq 0 \end{pmatrix} \end{pmatrix}\wedge \quad (3.10)$$

$$Is\ Acc\ AL\ By\ PIS\left(U,OWR,PIS\right),$$

Мұндағы Ass – қолжетімділік;

Ri – ЖОО АББО АР-ға қолжетімділік құқығы;

AL – рұқсат;

TRU – сенімді;

$MapU$ – абоненттің (қолданушының) картасы;

$ListU$ – абоненттің жергілікті есептік жазбасы;

$MapU\ To\ UD$ – АР иесінің -OWR жергілікті есептік жазбалары форматында ЖОО АББО АР қолданушылардың жиынын көрсететін функция.

ЖОО АББО үшін нақты киберқауіпті жүзеге асыруға мүмкіндік беретін (өкілеттіктің (құқықтар жиынтығының) шектеуін бұзу) ықтимал параметрлерін табуға болады және осы параметрлердің көмегімен барлық АҚЖ-ның жұмысын модельдеуге болады деп қабылданды. Сонымен қатар, сәйкес келетін ықтимал Петридің желілерінде (ЫПЖ) немесе Петри-Марков желілерінде (ПМЖ) таңбалардың ауысудың ықтимал параметрлері және ауысу ықтималдығы есептелінеді [77,78].

Бұдан әрі, ЫПЖ немесе ПМЖ траекториялары бойынша жарты қадаммен қозғалуды талдаймыз. ЖОО АББО-да қатерді жүзеге асыру- бұл ЫПЖ немесе ПМЖ бойынша қозғалу тәртібі (жарты қадамдар). ЫПЖ-да немесе ПМЖ-да әрбір күйі қандай да бір кездейсоқ уақыт аралығында сақталады деп ойлаймыз. Қарастырылып отырған уақыт аралығына тағы да ықтималдықтың таралу тығыздығының шамасын беретін параметрді сәйкестендіріп қоямыз. Бұдан әрі, ЫПЖ немесе ПМЖ траекториялары бойынша жарты қадаммен қозғалуды талдаймыз. Ары қарай келесі күйге ЫПЖ-да немесе ПМЖ-да ауысудың логикалық шарттарын тексереміз. ЫПЖ-дағы немесе ПМЖ-дағы күйлердің тұрақтылығы қарастырылып отырған киберқатер үшін зерттелетін процестің траекториясын анықтайды. Бастапқы күйден соңғы күйге дейін қозғалу

траекторялары үшін интегралды-дифференциалдық теңдеулерді қолданып процесті аналитикалық түрде сипаттауға болады [64].

Мысал қарастырайық: айталық $h(tr:1(a)) \to j(a) = h(tr_1) -$ $a_{1(a)}$ күйден (әрпі бар индекс, күйдің нөмірін білдіреді) $a_{j(a)}$ күйге қозғалу траекториясының нөмірі.

Траектория жарты қадамдар сериясын қамтиды. Немесе күйден ауысуға, содан кейін ауысудан күйге және т. б.:

$$S_{1[h(tr)]}, S_{2[h(tr)]}, \ldots, S_{i[h(tr)]}, \ldots, S_{j[h(tr)]},$$

мұндағы i, j – индекстер, күйдің нөміріне (немесе ауысу нөміріне) сәйкес келеді.

Траекториялар саны $H(tr)$ шамамен сипатталған. Онда сәйкес келетін жарты қадам орындалатын уақытты бөлу ықтималдығы мен тығыздығын беретін шамалар сәйкесінше $P_{j(a)j(z)}$ және $f_{j(a)j(z)}$ болады.

$h(tr_{1j})$ бойынша $a_{1(a)}$ ден $a_{j(a)}$ ге қозғалу уақытын бөлу ықтималдығы мен тығыздығын былай табамыз [66]:

$$P_{h(tr_{1j})} = \prod_{j[h(ttr_{1j})]=1}^{J[h(tr_{1j})]} P_{j[h(tr_{1j})]};$$

$$f_{h(tr_{1j})} = f_{1[h(tr_{1j})]} * f_{2[h(tr_{1j})]} * \ldots *$$
$$* f_{i[h(tr_{1j})]} * \ldots * f_{J[h(tr_{1j})]},$$

мұндағы $J[h(tr_{1j})]$: $h(tr_{1j})$ траекториясындағы позициялар мен ауысулар саны;

$*$ - барлық мүмкін болатын $h(tr_{1j})$ бойынша $a_{1(a)}$ орам операциясын белгілеуі мына қатынастардан:

$$P_{1(a)j(a)} = \prod_{h(tr_{1j})=1}^{H(tr_{1j})} P_{h(tr_{1j})}; \qquad (3.11)$$

$$f_{1(a)j(a)} = \frac{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} P_{h(tr_{1j})} \cdot f_{h(tr_1)}}{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} P_{h(tr_{ij})}}. \qquad (3.12)$$

[76] сәйкес ЖОО АББО-да қаралатын киберқауіпсіздігін жүзеге асыру мүмкіндігінің $\Phi_{i,j(t)}$ ықтималдығын табуға болады.

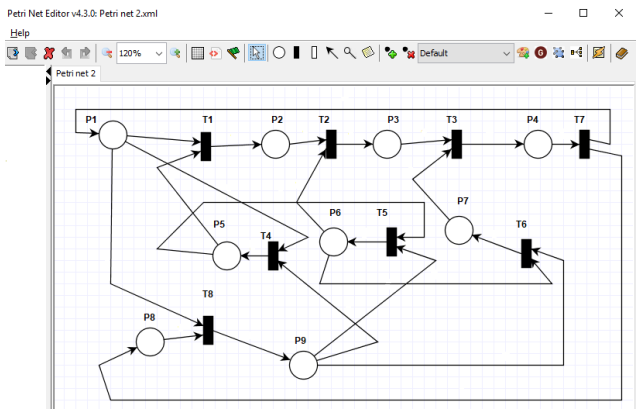
Жұмыстарды [65-72] есепке ала отырып, ЖОО АББО желісінің ерекшеліктерін ескере отырып, қолжетімділікті бақылау және басқару (ҚББ) тәсіліне нақтылау енгізу ұсынылды. ҚББ нақтыланған және толықтырылған тәсіл қауіпсіздік саясатының міндеттерімен және талаптарының сұранысы бойынша қолжетімділік құқықтарын салыстырудан сонымен қатар, ЖОО АББО-дағы қолжетімділікке рұқсат етілген төбелерді бекітуді келісуден тұрады.

ЖОО АББО төбелері үшін өздеріне тиісті құқықтары бар, барлық абоненттер үшін қолжетімділік құқықтарын салыстыру процедурасы жүргізіледі. Нәтижесінде абоненттік есептерді орындауға рұқсат етілетін төбелер жиыны алынады. Бұл ретте нақты ЖОО АББО үшін қауіпсіздік саясатының ағымдағы көрсеткіштері және қауіпсіздік метрикасы ескеріледі. Жаңа тапсырмалар немесе қайта бөлуге болатын тапсырмалар үшін ережелерге нақтылаулар енгізуге болады. Бұл, тапсырмаларды нақтылау немесе қайта қарастыру Петри желілерінің шартты белгілері (3.8)–(3.10) өрнектермен берілген математикалық модельді ескере отырып сипатталуы мүмкін.

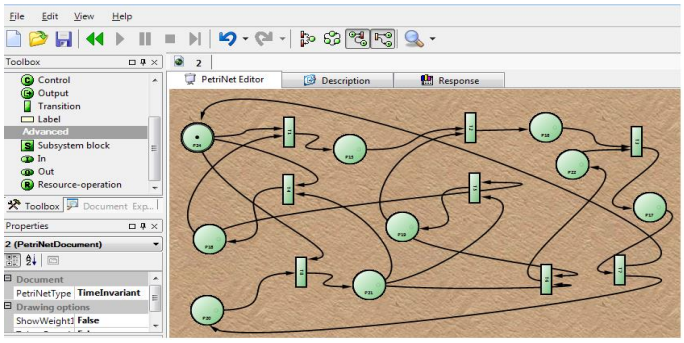
Жоғарыда келтірілген пайымдауларға сүйене отырып, Петри модификацияланған желілерінің (ПМЖ) негізінде ЖОО АББО ресурстарына қолжетімділікті бейімделген рөлдік басқару моделі құрылды (Қолжетімділікті басқару жүйесі- ҚБЖ) және PIPE v4.3.0 (PlatformIndependentPetrinetEditor) және Petri.NetSimulator. 2.017 пакеттерінде имитациялық модельдеу орындалды. Мұндай тәсіл даулы жағдайларды адекватты сипаттауға мүмкіндік берді, сонымен қатар, қолданушылары көп жұмыс режимі процесінде ЖОО АББО-да көптеген АЖ пайда болатын сұраныстарды өңдеу ерекшелігі ескерілді.

Имитациялық модельдер схемалары (сұлбалары) және модельдеудің формальды нәтижелері көрсетілген (суреттер 16,17,18).

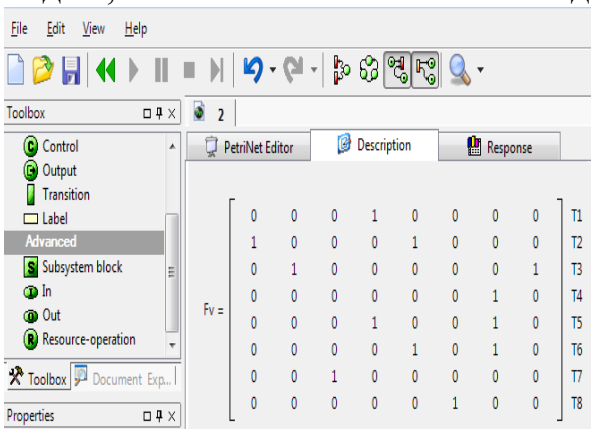
Схемалар қолжетімділік құқықтары жүйесінің операциялық моделінің логикалық құрылымын көрсетеді (үш сатылы басқару нұсқасы үшін). ПМЖ негізінде құрылған желілік модельдегі позициялар және ауысулар 7-кесте көрсетілген.



Сурет 16 - ЖОО АББО-да қолжетімділікті бейімделген басқарудың имитациялық моделі (абоненттің рөлін реттеуді ескере отырып), Pipe v4.3.0 модельдеу ортасы



Сурет 17 - ЖОО АББО-да қолжетімділікті бейімделген басқарудың имитациялық моделі, Petri.NetSimulator. 2.017 модельдеу ортасы



Сурет 18- ЖОО АББО-да қолжетімділікті бейімделген басқару моделіндегі позицияларды формальдау Petri NetSimulator. 2.017 модельдеу ортасы

Зерттеу процесінің барысында ұсынылған модельдердің нәтижелілігін бағалау және қолжетімділік құқықтарын бақылау әдісін нақтылау орындалды.

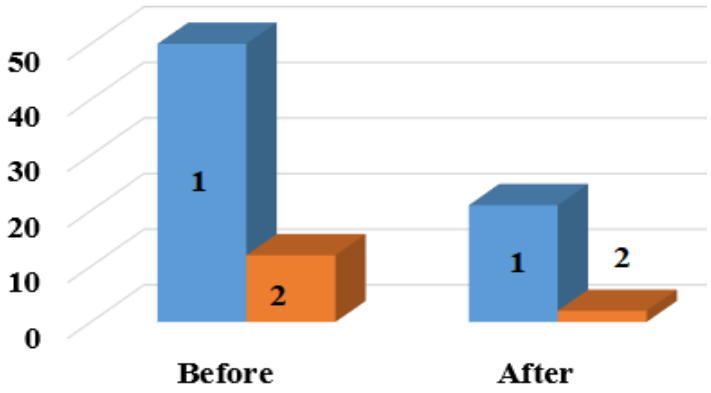
Ұсынылған шешімдердің нәтижелілігін бағалау үшін шешім қабылдауға кеткен уақыт шығынын қысқартуды сипаттайтын көрсеткіш қолданылды. Сәйкесінше, ұсынылған модельдер мен әдісті қолданғанға дейін және қолданғаннан кейінгі мәліметтерді өңдеуге кететін уақыт шығындары бағаланды.

Имитациялық эксперимент 400 есептеу төбелері үшін жүргізілді. Әрбір төбеге бір виртуалды машина сәйкес қойылды. ЖОО АББО-да АҚ және КҚ интеграцияланған жүйесіне имплементацияға дейін және оны енгізгеннен кейін жүзеге асырылған киберқатер саны көрсетілген (сурет 19).

Имитациялық модельдеу барысында алынған статистикалық мәліметтер (атап айтқанда, ПМЖ-дағы маркерлердің динамикасына қатысты) модельді сынаққа қатысқан компаниялар үшін, ҚБЖ-де нақты сипаттамаларды белгілеуге негіз берді.

Кесте 7 - Имитациялық модельде қабылданған белгілеулер (жетілдірілген Петри желілері негізінде)

Позициялар	
Схемада қабылданған белгілеулер (сурет 16,17)	Қолданушыға арналған позицияның сипаттамасы
*P*1	белсенді күй
*P*2	Абонентке жоба бойынша жұмыс істеуге рұқсат берілді
*P*3	Абонентке ЖОО АББО-ның функционалдық компоненттерімен (ФК) жұмыс істеуге рұқсат берілді
*P*4	Абоненттің ЖОО АББО-ның файлдары мен контентіне рұқсаты бар
*P*5	Тапсырмаларды орындау үшін қолжетімділік құқығын тексеру
*P*6	ФК-ға қолжетімділік құқығын тексеру
*P*7	ЖОО АББО-ның файлдарына қолжетімділік құқығын тексеру
*P*8	ҚБЖ –ның бастапқы күйіне қайта келуі
*P*9	Әрекет ету уақытын шектеу (мысалы, тапсырманы нақтылау немесе тест тапсырмаларын орындау кезінде)
Ауысулар	
Белгілеулер	Сипаттамасы
*T*1...*T*8	Маркерлердің желідегі бір позициядан екінші позицияға ауысу (және модификациялау) шарттарының жиынын көрсетеді. Шарттар априорлық (алдыңғы) мәліметтер жиынынан анықталған.



Сурет 19 - ЖОО АББО-ның ақпараттық қауіпсіздігін бағалау

Суреттегі белгілеулер: 1- ЖОО АББО –да жүзеге асырылған киберқатерлердің жалпы саны; 2- қолжетімділік құқықтарын бұзуға және өкілеттіктерін асыра пайдалануға байланысты киберқатерлер.

Біз қолданған тәсілдің артықшылықтарына ұсынылған шешімдер, атап айтқанда, Петри желілерінің аппаратын пайдалана отырып құрылған қолжетімділік құқықтарын бейімделген басқарудың тұжырымдамалық моделі, сондай-ақ модельдер мен әдіс Украина мен Қазақстанның бірнеше ірі жоғары оқу орындарының ақпараттық қауіпсіздік және киберқауіпсіздікті басқаратын ішкі жүйесінде (ЖОО АББО-ның ішкі жүйесі) сынақтан табысты өткен фактісін жатқызуға болады. Ұсынылған шешімдер негізінде құрылған бағдарламалық жабдықтар, ЖОО АББО-ның желілері абоненттерінің есептік жазбаларын бақылауды, сүйемелдеуді және өзгертуді автоматтандыруға мүмкіндік берді. Сонымен қатар, осы бағдарламалық жабдықтарда (атап айтқанда, «Қатерлерді талдау» [79] жүйесі) абоненттердің ақпараттық ресурстарға қолжетімділіктің деңгейін баптау арқылы, оны күрделендіру мүмкіндігі қарастырылған.

Келешекте зерттеуді жалғастыру ЖОО АББО-ның АҚ-ны және КҚ-ны талдауға байланысты, атап айтқанда, өте маңызды компьютерлік жүйелер мен ақпараттандыру нысандарында қолжетімділікті басқару және бақылау міндетімен байланысты, қолданбалы есептерді шешу үшін, келесі алгоритмдеу процестері үшін алынған нәтижелерді қолдану мүмкіндіктерімен анықталады.

3.2 Жоғары оқу орынының электрондық ақпараттық білім беру ортасына қолданушыларды аутентификациялау кезінде мүмкін қатерлерді талдау әдісі мен моделі

1-тарауда көрсетілгендей, абоненттердің іс-әрекетін тексерудің қате нәтижелерін азайту есептеріне назар аудару кезінде, ЖОО-ның электрондық ақпараттық білім беру ортасына рұқсат етілмеген қолжетімділік (РЕҚ) қатерлерін анықтайтын қолданыстағы әдістері мен модельдерін жетілдіру және жаңа әдістер мен модельдерді құру бойынша міндеті өзекті болып қала береді. Бұл

ЖОО АББО-да жаңа қатерлерді анықтаудың нәтижелілігін және жоғары оқу орындарының АҚЖ-ны, киберқауіпсіздіктің ресурстарын тиімді бөлуді арттыруы тиіс.

Нәтижелері диссертацияның осы бөлімінде ұсынылған зерттеудің мақсаты, жоғары оқу орнының электрондық ақпараттық білім беру ортасында абоненттерді аутентификациялау кезінде РЕҚ қатерін анықтау процедурасына қатысты қолданылатын әдістер мен математикалық модельдерді дамытудан тұрады.

Мақсатқа жету үшін дамыту және құру бойынша есептер шешілді:

– ЖОО АББО-дағы мүмкін қатерлері туралы мәліметтерді талдау әдісі, бұл әдіс қатерлерді тануға кететін уақытты барынша азайтуға мүмкіндік береді;

– жаңылыс іске қосылулар және жалған қатерлер туралы хабарламалар санын қысқартуға мүмкіндік беретін, ЖОО АББО абоненттерін аутентификациялаудың математикалық моделі.

ЖОО АББО үшін қатерлерді детекторлауға қатысатын жиынтығын (бұдан әрі ҚДЖ – қатерді детекторлау жиынтығы) қалыптастыру кезінде мыналар ескерілді:

– детектор абоненттердің (ЖОО АББ-ның қолданушылары) іс-әрекеттері кезінде іске қосылмауы керек. Сондай-ақ, детектор ЖОО АББО-да ақпаратты қорғау және КҚ жүйелерінің нысандары мен субъектілерінің заңды іс-әрекеттері кезінде іске қосылмауы керек; детекторлау нысандарына сәйкес келетін, белгілердің жүзеге асырылу мәндерінің интервалдары, тепе-теңдігін азайту үшін жеткілікті болуы тиіс, детекторлау жүйесін оқыту үшін қолданылатын нысандар [74,75] зерттеу жұмыстарында сипатталған модельдер мен әдістерді пайдалана отырып қабылданды;

– егер ЖОО АББО үшін қатерді детекторлауға қатысатын жиынтықтың бір экземпляры оны сәтті таныса, онда бұл экзепляр АҚЖ-ның білім базасында сақталады және бұдан әрі КҚ жүйелерін «жаттықтыру» үшін қолданылатын нысандардың жаңа буынын қалыптастыруға қатысады.

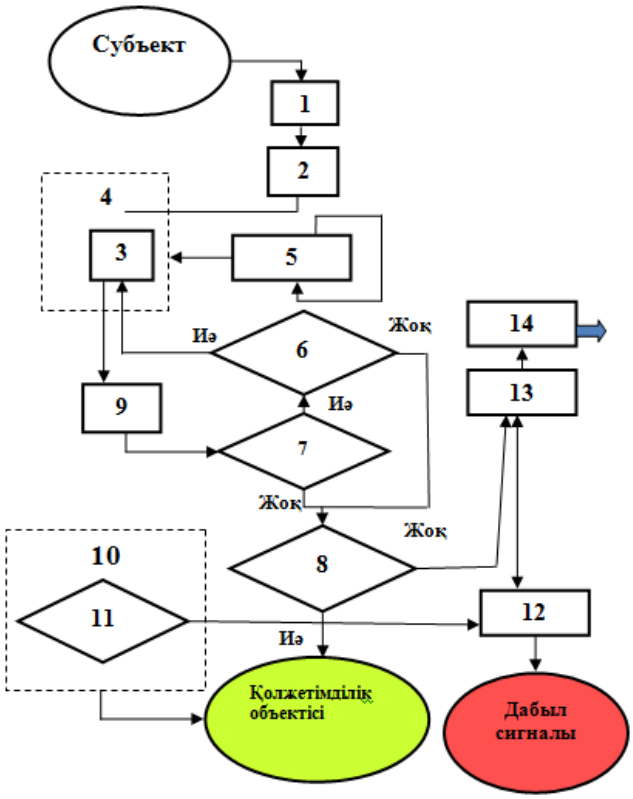
ЖОО АББО абоненттерін аутентификациялаудың қолданыстағы әдістері мен алгоритмдерін талдай отырып, жетілдірілген схема құрылды (сурет 20).

Схемада екі жиын пайдаланылады. №1 жиын ЖОО-ның нақты АББО АҚЖ-ның білім базасында бұрын кездескен қатерлерді базадан іздеуге арналған. №2 жиын жаңа қатерлерді анықтауға арналған.

ЖОО АББО-ның субъектісін аутентификациялау кезінде бұрын кездеспеген қатерлерді жаңа деп түсінеміз. Ұсынылған схеманың ерекшелігі салыстыру процесін іске қосу мүмкіндігінде. Бұл тәсіл «жақын» ҚДЖ- ны белсендіруші сигналды алуға негізделген. Бұл ретте сигналды талдау кезінде ЖОО АББО-да бір субъектісі ұсынған мәліметтердің барлық массиві қолданылады.

Схемада қабылданған белгілеулер: 1-субъектінің сәйкестендіруші мәліметтерін оқу; 2 –іздеу үшін ұсынатын жиынтықты құру; 3- қатерлерді детекторлау үшін пайдаланылатын жиынтықтар жиынында (ҚДЖЖ) іздеу

процедураларын іске асыру; 4-ЖОО АББО-да қатерлерді детекторлау үшін пайдаланылатын жиынтықтар жиыны; 5 – ҚДЖЖ-ны жаңарту; 6-сигналды тексеру; 7-растау сигналын күту; 8-тексеру өтті; 9-қорытынды мәліметтерді қалыптастыру; 10-қатерлерді детекторлау үшін пайдаланылатын жадыдан қалпына келтірілген жиынтықтардың жиыны; 11-қатерлерді детекторлау үшін пайдаланылатын жадыдан қалпына келтірілген жиынтықтардың жиынының ішінен іздеу; 12-субъектінің іс-әрекеттерін бұғаттау; 13-ЖОО АББО-ны қорғау жүйесінің жадына жазу; 14-жадыны жаңарту.



Сурет 20- Жаңартылған ҚДЖ негізінде ЖОО АББО субъектісін аутентификациялау схемасы

ЖОО АББО жаңартылатын ҚДЖ (бұдан әрі-ЖҚДЖ) негізінде субъектіні аутентификациялаудың ұсынылған схемасы үшін кіру әрекетін анықтауға болатын жылдамдықты есептеу үшін келесі теңдеулер қолданылды (сурет 21):

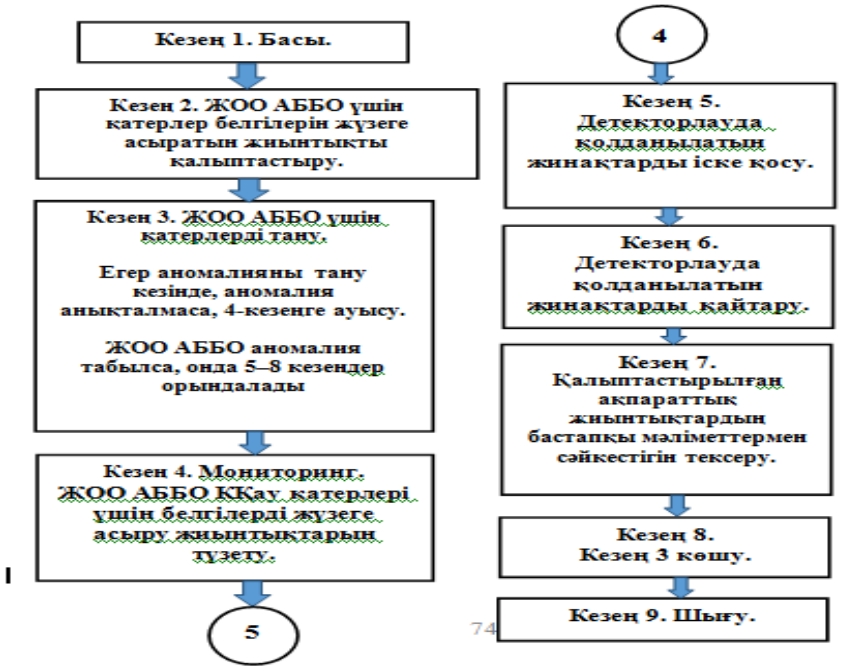
$$\frac{da}{dt} = rev \cdot \zeta \cdot |Tr| - \alpha \cdot |Tr(MP \setminus W(MP))|, \quad (3.13)$$

$$W(MP) = \{w \mid \forall w \exists mp \in MP : (w)\, Con\, MP\}, \quad (3.14)$$

мұндағы $Tr = Tr(S)$ – ЖОО АББО үшін қатерлер жиыны; MP – ЖОО АББО-ның ақпаратты қорғау жүйесі; $W(MP)$ – абоненттерді тексерулерге тартылған

АҚЖ, rev – ЖОО АББО-ны ақпаратты қорғау жүйесі іске қосылған кезіндегі кідіріс коэффициенті; ζ – қатерлер санының ұлғаюын сипаттайтын коэффициент; $Tr(PR)$ – АҚЖ залалсыздандырылған қатерлер; α – шабуыл жасалғаннан кейін ЖОО АББО-ның жұмысқа қабілеттілігінің бұзылу дәрежесін сипаттайтын коэффициент; Con – ЖОО АББО үшін қорғау жүйесімен залалсыздандырылған қатерлер болған кездегі шарттар.

ЖОО АББО-ның мүмкін қатерлер туралы мәліметтерді талдаудың ұсынылған әдісі схемалық түрде көрсетілген (сурет 21). Жұмыс [72] нәтижелерін есепке ала отырып ҚДЖ «жаттығу» процесінде, «себеп-салдар» ерекше айқын байланысы бар ЖҚДЖ үшін салмақты мәндерді қолдану ұсынылды. ЖОО АББО үшін қатерлерді анықтаудың нәтижелілігін арттыру есептерінің басымдылығы тұрғысынан, рұқсат етілген облысқа енбеген ҚДЖ-ны алып тастау міндетті екені көрсетілген. Нәтижесінде, қатерлерді тану жүйесі мен тиісті алгоритмнің «жаттығулар» нәтижесі ретінде келесі жаттығуға қабілетті қорытынды ішкі жиын аламыз. Аутентификация процесінде авторизацияланған субъектілерден алынған мәліметтер пайдаланылады деп есептейміз. Сонымен қатар, ЖОО АББО-да мүмкін қатерлер туралы мәліметтерді талдау процесінде ҚДЖ, абоненттер туралы қызметтік мәліметтер және реттеуші ережелер енгізілген. Алгоритм басында ЖОО АББО-да АҚЖ-дан алынған мәліметтер қолданылады (мысалы, бастапқы ақпарат субъектіден алынады). Бұдан әрі ҚДЖ осы ақпаратты тексереді және тиісті шешімді құрайды.



Сурет 21- ЖОО АББО үшін қатерлерді детекторлауға қатысатын жиынтықтарды қалыптастыру тізімі

Төменде жоғары оқу орнының электрондық ақпараттық білім беру ортасында қолданушыларды аутентификациялау кезінде мүмкін қатерлерді талдау ішкі жүйесі үшін реттеуші ережелердің мысалы келтірілген.

Мынадай бастапқы мәліметтер берілген:

DS – ҚДЖ жиыны $(ds \in DS)$;

ID – ЖОО АББО субъектісінен бастапқы ақпарат $(id \in ID)$;

SS – ҚДЖ белгілерін немесе субъектінің бастапқы мәліметтерін жүзеге асыру жиыны;

VE – t уақыт кезеңіндегі тексеру нәтижелері;

SP – ЖОО АББО АҚЖ қызметтік параметрлері.

ЖОО АББО мәліметтер базасын басқару жүйесі үшін реттеуші ережелердің келесі тізімі алынды (абоненттерді аутентификациялау моделі):

$$VE(ds(ID)) = \sum(all\ SS(id) > tv(SS)); \qquad (3.15)$$

$$if \quad VE(ds(ID)) > tvr \quad \& \quad nc = isNull \quad then$$
$$VE = 1 \quad \& \quad new\ ds(ID); \qquad (3.16)$$

$$if \quad VE(ds(ID)) > tvr \quad \& \quad nc == 0 \quad then$$
$$VE = 0 \quad \& \quad Stop; \qquad (3.17)$$

$$if \quad VE(ds(ID)) > nc \cdot tvr \quad then$$
$$ds(nit) \subset new\ DS, \qquad (3.18)$$

мұндағы tv – бастапқы мәліметтермен берілген белгілерді жүзеге асыру жиынтығының (SS) ұқсастықты салыстырудың межелік деңгейі;

tvr – ЖОО АББО үшін қатерлер туралы ескертуді тіркейтін ҚДЖ-ның қорытынды мәліметтерінің межелік деңгейі;

nc – басқа (екінші, үшінші және т. б.) ҚДЖ -ға тексеру кезінде қатер шынымен расталды және nc - расталудың ең аз саны (субъектіні потенциалды қауіп төндіретіндердің қатарына жатқызу үшін міндетті);

nit – циклдегі итерация саны.

Ұсынылған аутентификация схемасында пайдалануға болатын элементтердің келесі түрлері қарастырылды:

№ 1 топ - детекторлау процестеріне қатысатын жиындар (мысалы, жиынтықтарды оқыту нысандары ретінде қолданылатын бинарлы матрицалар). Әрбір жиынтық бақылау нысандарының белгілерін жүзеге асырудың нақты класына сәйкес келеді [75]. Бірінші топ ЖОО АББО-ның субъектісі ұсынған ақпаратты өңдеуге жауап береді.

№ 2 топ - ЖОО АББО-ның базалық нысандары (БО). Қорғалатын ЖОО АББО әрбір элементі үшін (бірқатар жағдайларда барлық жүйе үшін) ішкі БО жиынын қалыптастырады. Бұл БО қызметтік функцияларды жүзеге асыруға арналған.

ЖОО АББО-ның стандартты БО-ға мыналарды жатқызуға болады: ақпараттық массивтер, сондай-ақ қорғау нысанын өзіндік сипаттамалары бойынша мәліметтерді қамтитын, жазып алатын және жинайтын нысан болады. Бұл ақпарат кейін қатерлерді детекторлауға қатысатын жиынтықтарды біріктіру үшін негіз ретінде пайдаланылатын болады. Екінші топқа, сондай-ақ ЖОО АББО-ны қорғау жүйелерінің қызметтік конфигурацияларын жатқызуға болады. Бұл конфигурациялар қатерлерді детекторлауға қатысатын жиынтықтарға нақтылау енгізу үшін міндетті мәліметтерді қамтиды.

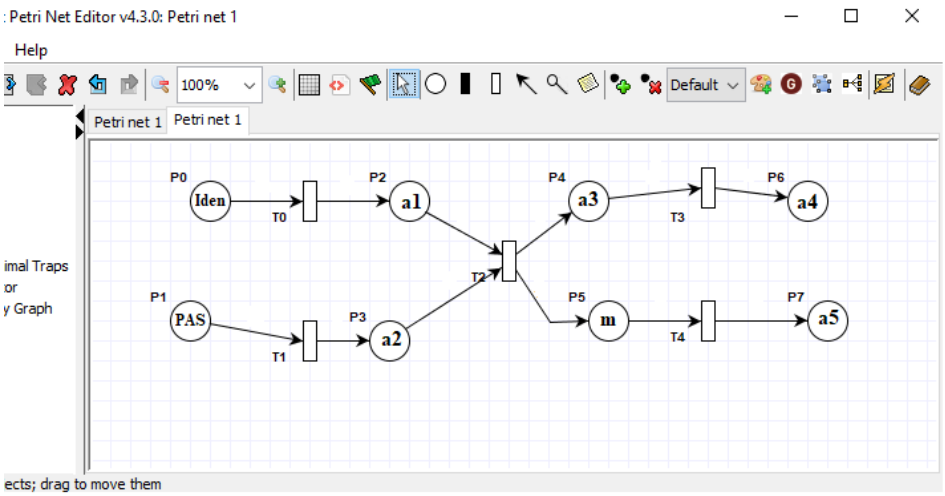
ЖОО АББО-ның басқарушы ішкі жүйесі туралы да атап өткен жөн. Бұл ішкі жүйе ЖҚДЖ негізінде ЖОО АББО-ны клавиатуралық тану процесінде субъектілерді аутентификациялау процесін бақылауды тікелей жүзеге асырады.

Ұсынылған әдіс мынадай мүмкіндік береді:

1) верификация нәтижелерінің дәлдігі мен сенімділігін арттыру (бұл ЖОО АББО-ны қолдану барысында қосымша тексерулер есебінен қол жеткізілді);
2) ЖОО АББО-ның нақты киберқатер кластастары үшін ҚДЖ жиынтықтарының ақпараттылығын арттыру (бұл ҚДЖ-ға бөлінетін белгі кеңістігін барынша азайту үшін жоғары дәрежелі қатер белгілерінің мәндерін сақтау есебінен қол жеткізілді).

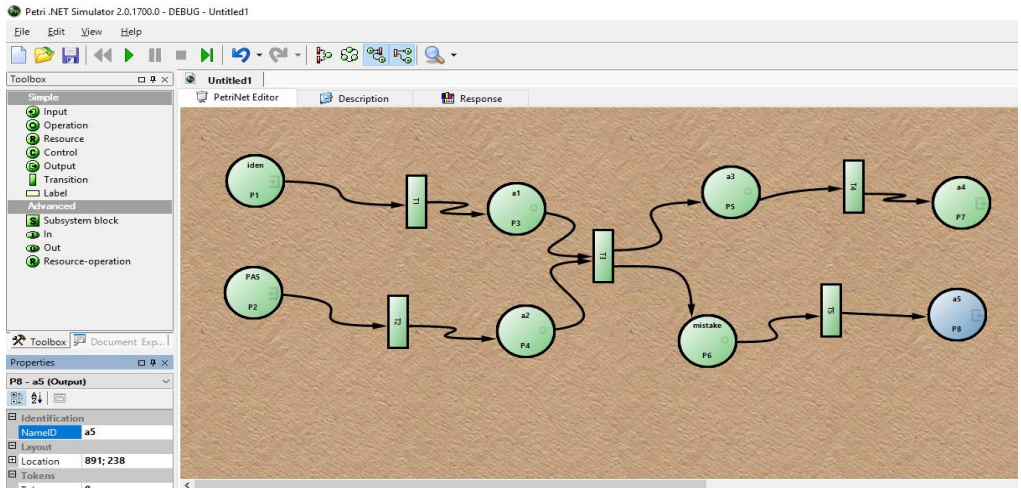
ЖОО АББО-ға кірген кезде қолданушыларды идентификациалаудың (аутентификациялау) классикалық нұсқасы пароль арқылы жүргізіледі. ЖОО АББО ресурстарын қолданушылар мәліметтерді енгізе алады, өзгерте алады, мысалы, оқу тапсырмаларына жауаптарды жүктеу кезінде немесе басқа жағдайларда.

Pipe v4.3.0 ортасында имитациялық модельдеуді идентификацияның (аутентификация) классикалық схемасы үшін орындайық. Алгоритмнің блок-схемасы және классикалық схема үшін қолданушының ЖОО АББО-ға кіру Петри желісі ұсынылған (сурет 22). Осыған ұқсас модель Petri.NetSimulator. 2.017. ортасында көрсетілген (сурет 23).



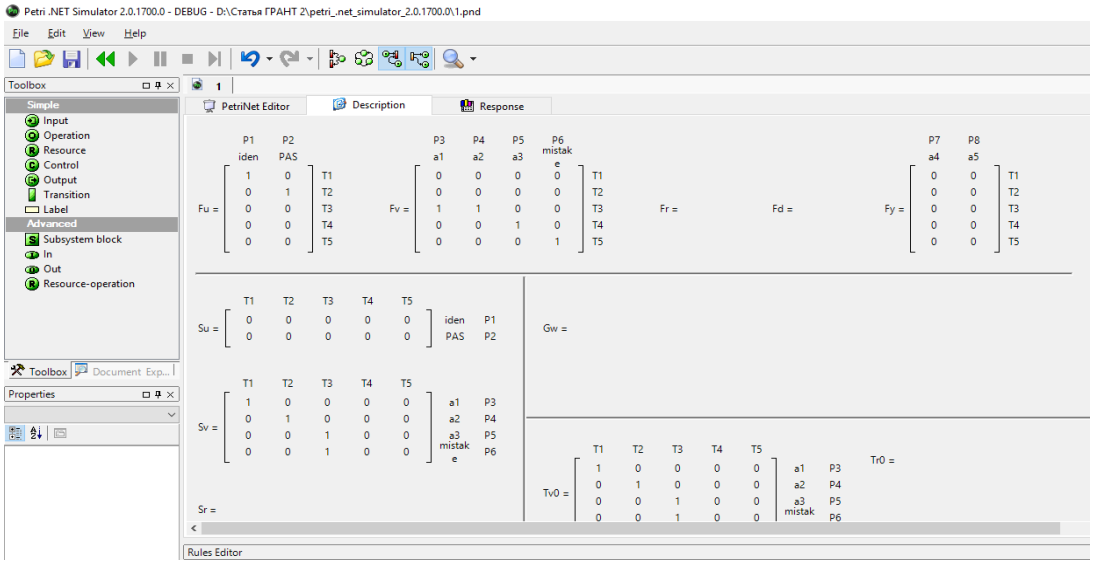
Қабылданған белгілеулер: $P1(PAS)$ – аутентификация үшін ЖОО АББО желісіне абонент енгізетін пароль (талаптарға сәйкес келетін пароль; басқа түрдегі фишкалар - дұрыс емес және (немесе) қисынсыз парольдар); $P0(Iden)$ – ЖОО АББО-да идентификация үшін қолданушы пайдаланатын идентификатор; $a1$ – ЖОО АББО сұранысы бойынша парольды енгізу; $a2$ – абонент (қолданушы) енгізген идентификатор; $a3$ – идентификатор пароль тексеруінен өтті және аутентификация сәтті аяқталды; $a4$ – ЖОО АББО қолданушының рұқсат етілген кіруі; $a5$ – ЖОО АББО қолданушының қолжетімділік құқығы берілмеген; $T0-T4$ – ауысу шарттарының жиынтығын көрсетеді.

Сурет 22- идентификацияның (аутентификация) классикалық схемасы үшін қолданушының ЖОО АББО-ға кіру Петри желісі, pipe v4.3.0 ортасы



а) желі моделі

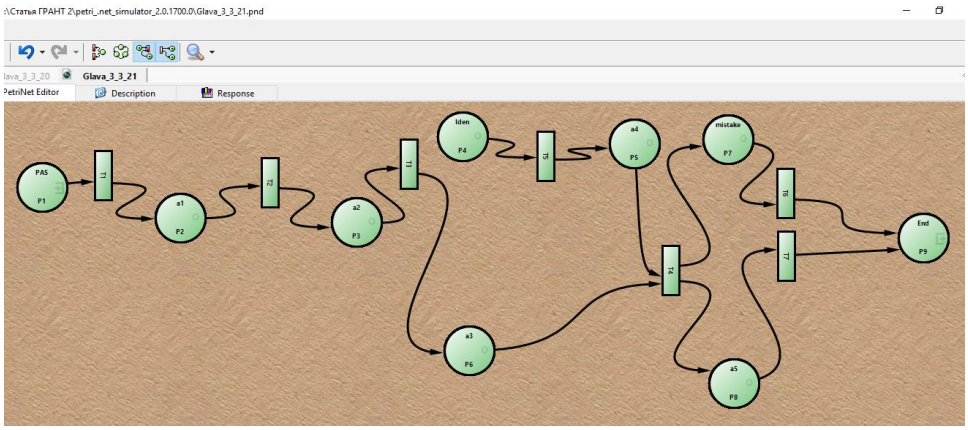
Сурет 23- идентификацияның (аутентификация) классикалық схемасы үшін қолданушының ЖОО АББО-ға кіру Петри желісі, Petri NetSimulator. 2.017 ортасы, бет 1



б) модельдеу нәтижелерінің үзіндісі

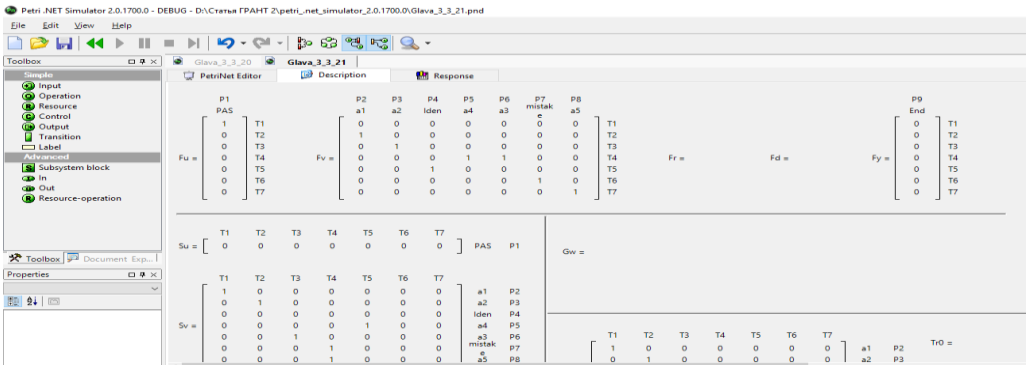
Сурет 23- идентификацияның (аутентификация) классикалық схемасы үшін қолданушының ЖОО АББО-ға кіру Петри желісі, Petri NetSimulator. 2.017 ортасы, бет 2

Бұрын құрылған схеманы басшылыққа ала отырып (сурет 20,21), жаңартылған ҚДЖ негізінде ЖОО АББО-да субъектінің аутентификация схемасы үшін имитациялық модельдеуді орындаймыз (сурет 24).



а) желі моделі

Сурет 24- Петри желілерінің шартты белгілерін пайдалана отырып, жаңартылған ҚДЖ негізінде ЖОО АББО-да субъектіні аутентификациялау схемасы үшін имитациялық модельдеу (Petri.NetSimulator. 2.017.), бет 1



б) модельдеу нәтижелерінің үзіндісі

Сурет 24- Петри желілерінің шартты белгілерін пайдалана отырып, жаңартылған ҚДЖ негізінде ЖОО АББО-да субъектіні аутентификациялау схемасы үшін имитациялық модельдеу (Petri.NetSimulator. 2.017.), бет 2

8-кестеде жаңартылған ҚДЖ негізінде ЖОО АББО-да субъектіні аутентификациялау схемасы үшін имитациялық модельде қабылданған белгілеулер көрсетілген (Петри желілерінің негізінде ұсынылған) (сурет 24).

Кесте 8 - Жаңартылған ҚДЖ негізінде ЖОО АББО-да субъектіні аутентификациялау схемасы үшін имитациялық модельде қабылданған белгілеулер

Позициялар	
Схемада қабылданған белгілеулер (сурет 24)	Қолданушыға арналған позицияның сипаттамасы
PAS	аутентификация үшін ЖОО АББО абоненті енгізген пароль
Iden	ұсынылған жиынты тексеру
*a*1	ЖОО АББО-да сұраныс кезінде парольді енгізу
*a*2	абонент (қолданушы) енгізген идентификатор детекторлық жиынтықтың (ДЖ) "эталонымен" сәйкес келеді
*a*3	ҚДЖ абонент енгізген идентификатор ДЖ "эталонмен" сәйкес келетінін анықтады
*a*4	ҚДЖ абонент енгізген пароль ДЖ "эталонымен" сәйкес келетінін анықтады
*a*5	ЖОО АББО абоненті тексеруден өтті
mistake	тексеру аяғына дейін өткен жоқ, ЖОО АББО-да қорытынды мәліметтерді қалыптастыру және ҚДЖ-ны нақтылау қажет.
Ауысулар	
*T*1...*T*7	Маркерлердің желінің бір позициясынан басқасына ауысу шарттарының (және модификациялау) жиынтығын көрсетеді. Шарттар априорлық мәліметтер жиынтығымен анықталған.

ЖОО АББО-да субъектінің іс-әрекетін талдау есебі үшін ұсынылған аутентификация сызбасы есептеу эксперименттерін және білікті тексерулерді салыстыру барысында алынған қорытынды мәліметтердің жиынтығының үзіндісі көрсетілген (кесте 9).

б) жағдайда ЖОО АББО-да субъектінің іс-әрекеттерін талдау есебі үшін ұсынылған аутентификация сызбасының тестілеу нәтижелері көрсетілген (сурет 24). Графиктерде ЖОО АББО-да паролді қорғау жүйесінің модуліне тәуелділіктер көрсетілген (сурет 25). Бұл ретте субъект енгізген символдар санынан ЖОО АББО-да субъектіні тану жылдамдығы талданады.

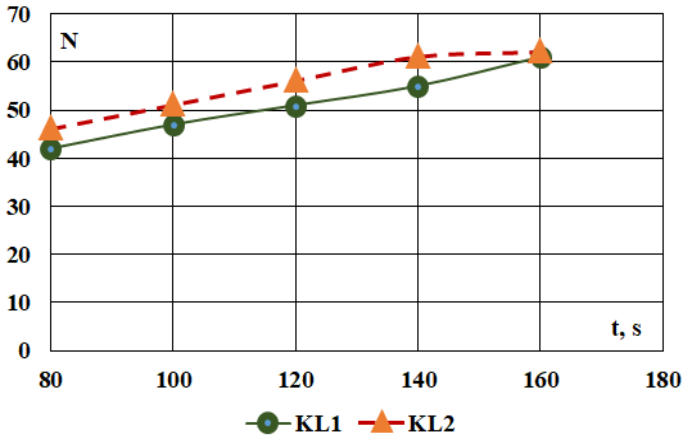
Кесте 9 - Эксперимент барысындағы қорытынды мәліметтер жиынтығының үзіндісі

$rev \cdot \cdot \zeta \cdot \cdot \lvert Tr \rvert$	t, s	ЖОО АББО-да потенциалды қауіпті субъектілерін анықтау ықтималдығы									
		ЖОО АББО-да субъектінің стандартты аутентификациясы ·100%		ЖҚДЖ негізінде ЖОО АББО-да субъектілерін аутентификациялау, ·100%							
		$\alpha = 0{,}1$	$\alpha = 0{,}9$	$\alpha = 0{,}1$				$\alpha = 0{,}9$			
				$P_m = 0{,}7$		$P_m = 0{,}98$		$P_m = 0{,}7$		$P_m = 0{,}98$	
				ξ							
				0,1	0,3	0,1	0,3	0,1	0,3	0,1	0,3
1	50	59,2	0,2	100	99,9	99,3	99,2	77,2	71	50,3	45,4
	160	59,2	0,1	60,1	59,9	59,1	59,1	0,8	0,4	0,2	0,1
10	50	61,3	0,4	99,9	98,1	98,4	96	77,3	70,9	50,3	49,8
	160	60,1	0,4	60, 2	59,1	60,2	59,7	0,6	0,3	0,3	0,1
Ескертулер: P_m – ҚДЖ мәліметтері мен субъект ұсынған мәліметтер қате теңестірілуінің ықтималдығы (жиынтықтардың ұқсастығының межелік шегі алдын ала анықталған); ξ – бірнеше қатерлердің түріне нақты ҚДЖ негізінде тексеру нәтижелерін қолдану мүмкіндігін сипаттайтын коэффициент.											

Эксперименттерде парольдің ұзындығы 8 символға тең, ал парольды енгізуге болатын әрекеттер саны 3 деп қабылданды. Детекторлауға тартылған жиынтықтардың саны 250 болды. Осылайша, қаскүнем парольді біліп алса да, оған авторизацияланған абоненттің машиналық үлгісін жасау, міндетті оған ұзақ уақыт бойы бақылау жүргізу және содан кейін ЖОО АББО-да жаттығуды өткізу қиынға соғатыны көрсетілді. Демек, ҚДЖ негізінде ЖОО АББО субъектісін аутентификациялаудың ұсынылған схемасы жүйеде абонентті индентификациялау есептері үшін жеткілікті тиімді.

Зерттеудің артықшылықтарына мына фактіні жатқызуға болады: ұсынылған шешімдер, атап айтқанда, аутентификациялау үшін құрылған бағдарламалық

модульдерді, [76-82] жұмыстарда ұсынылған зерттеулердің нәтижелерімен салыстырғанда, ақпараттық жүйелер мен кәсіпорындар желілерінде потенциалды қауіпті субъектілердің табылу ықтималдығы жоғары екенін, ал ҚДЖ-да желі абонент берген мәліметтермен қате салыстыру жасау ықтималдығы аз екенін көрсетті.



Сурет 25- ЖОО АББО-да субъектінің іс -әрекеттерін талдау есебі үшін ұсынылған аутентификация схемасының тестілеу нәтижелері (қашықтан оқыту жүйесі мысалында)

Суретте көрсетілген белгілеулер $KL1$ – ЖОО АББО ЖҚДЖ негізге ала отырып қолданып клавиатуралық тану процесіндегі субъектіні аутентификациялау; $KL2$ – субъект үшін қарапайым парольдер арқылы қорғау; N – ЖОО АББО-да субъектінің клавиатурамен жұмысы істеу кезіндегі ауысулар саны.

Ұсынылған шешімдер негізінде құрылған бағдарламалық өнімдер, Украинадағы екі ірі жоғары оқу орынының желілері абоненттерінің есептік жазбаларын бақылауды, сүйемелдеуді және өзгертуді автоматтандыруға мүмкіндік берді. Сонымен қатар, «қатерлерді талдаушы» бағдарламалық өнімінде ақпараттық ресурстарға абоненттердің қолжетімділік деңгейіне нақтылау енгізу мүмкіндігі бар және ЖОО АББО-да қолданушыларды аутентификациялау автоматтандырылған.

Зерттеулердің болашағы ЖОО АББО қорғалуын талдауға байланысты алынған нәтижелерді процестің кейінгі алгоритмдері үшін қолдану мүмкіндіктерімен анықталады. Сондай-ақ, білім беру мекемесінің АҚЖ және КҚ жүйесін детекторлаудың бағдарламалық-аппараттық құралдарынан жаңартылған мәліметтер жиынтығын өңдеудің селективті алгоритмін қолдану процесінде мүмкін киберқатерлер туралы мәліметтерді өңдеуді бағдарламалық автоматтандыру да мүмкін болады.

Сонымен қатар, диссертацияның 4-тарауында сипатталған, құрылған бағдарламалық өнімнің көмегімен 3-тарауда сипатталған модельдер мен әдістерді

ескере отырып, ЖОО АББО-ның киберқауіпсіздік құралын қаржыландырудың рационалды стратегиясын таңдауға болады.

Үшінші тарау бойынша қорытындылар

Үшінші тарауда мынадай нәтижелер алынды:

– Жоғары оқу орнының ақпараттық білім беру ортасының киберқорғауын бейімделген басқарудың тұжырымдамалық моделі сипатталған;

– Петри желілерінің аппаратын пайдалана отырып, қолданушылардың қолжетімділік құқықтарын бейімделген басқару міндеттерін шешудің мысалы қарастырылған. Оған сәйкес келетін модель жүзеге асырылды және PIPE v4.3.0 және Petri.NetSimulator. 2.017 пакеттерде имитациялық модельдеу орындалды;

– жоғары оқу орнының ақпараттық білім беру ортасында киберқатерді азайту немесе бейтараптандыру үшін қолданушының профилін нақтылау процедураларын автоматтандыру мүмкіндіктері көрсетілген;

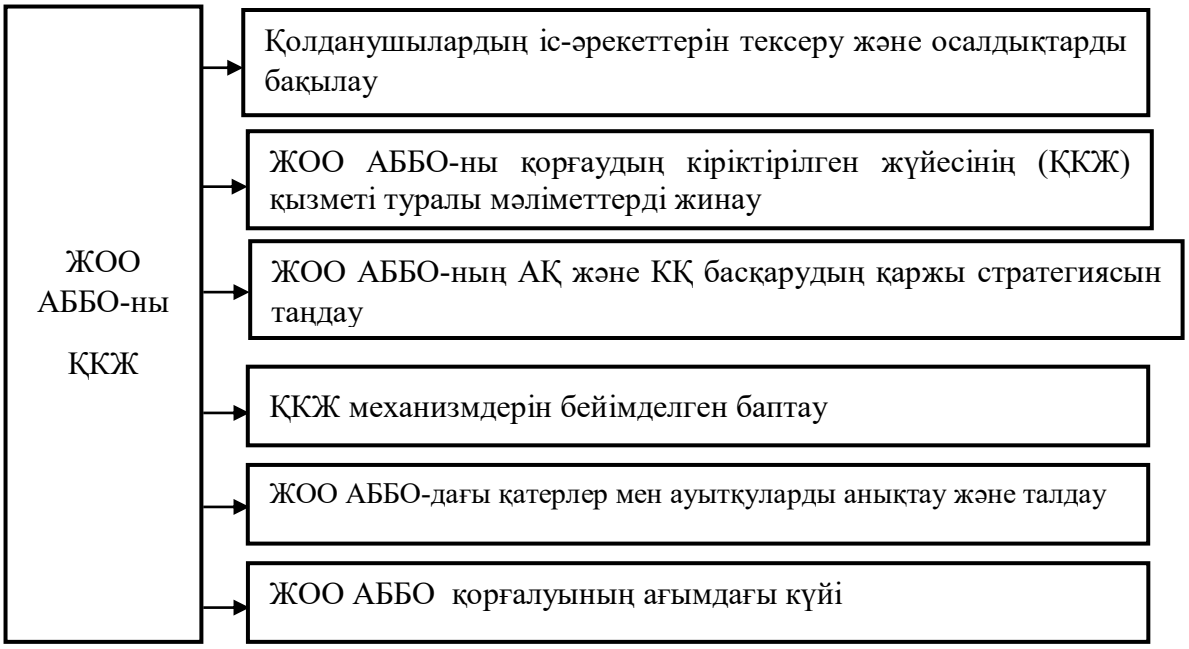
– ақпараттандыру нысандарының компьютерлік желілерінде қолданушылар тағайындаған есептерді үлестіру (міндеттерді бөлу) моделі сипатталған. Модель үшін база Петри желілерінің математикалық аппараты болды. Модельдің қолданыстағы модельдерге қарағанда айырмашылығы, бұл модельде күйдің ішкі кеңістігінің қуатын азайтуға мүмкіндік беретін айнымалылар бар. Сондай-ақ, модельдеудің нәтижелілігі, атап айтқанда қолжетімділік құқықтарын реттеуге байланысты шешімдер қабылдауға кететін уақыт шығындарын қысқарту есебінен жоғарылады;

– қолжетімділік құқықтарын бақылау әдісі нақтыланды және толықтырылды. Қауіпсіздік саясатының міндеттері мен талаптары сұранысының қолжетімділік құқықтарын салыстырып тексеру аспектілеріне қатысты нақтылаулар болды. Сонымен қатар, ЖОО АББО-ның міндеттері мен қолжетімділікке рұқсат етілген төбелердің сәйкестігі ескерілді. ЖОО АББО-ның төбелері үшін де тиісті құқықтары бар абоненттер үшін қолжетімділік құқығын салыстыру процедурасы қарастырылған. Модель жоғары оқу орнының нақты ақпараттық білім беру ортасы үшін қауіпсіздік саясатының ағымдағы көрсеткіштерін және соңғыларын нақтылау мүмкіндігі бар қауіпсіздік метрикасын ескереді. Жаңа міндеттер немесе қайта қарастырылатын міндеттер үшін қауіпсіздік ережелері мен метрикаларын нақтылау Петри желілерінің шартты белгілерінде сипатталған.

4 ЖОҒАРЫ ОҚУ ОРЫНЫНЫҢ АҚПАРАТТЫҚ БІЛІМ БЕРУ ОРТАСЫНЫҢ КИБЕРҚАУІПСІЗДІГІН ҚАРЖЫЛАНДЫРУ ЖҮЙЕСІНІҢ БАСҚАРУ МІНДЕТТЕРІН ОҢТАЙЛАНДЫРУДЫ БАҒДАРЛАМАЛЫҚ ЖАБДЫҚТАУ ЖӘНЕ ЖҮЗЕГЕ АСЫРУ

4.1 Жоғары оқу орынының ақпараттық білім беру ортасы киберқауіпсіздігінің кіріктірілген жүйесінің инвестициялауды басқару моделі

1-3 тарауларда ұсынылған зерттеулер нәтижелері жоғары оқу орнының АББО қорғаудың кіріктірілген жүйесінің құрылымдық схемасын қалыптастыруға мүмкіндік берді (сурет 26).



Сурет 26 - ЖОО АББО-ны қорғаудың кіріктірілген жүйесінің құрылымдық схемасы

Ұсынылған схема ЖОО АББО-ға кіріктірілген қорғауды бейімделген жағдайлық басқарудың мәнін көрсетеді. Сонымен бірге осындай кіріктірілген жүйенің басты мақсаты, ЖОО АББО абоненттері ЖОО-ның немесе басқа оқу орнының КҚ саясатын әдейі немесе байқаусызда бұзған жағдайларда ЖОО АББО-ның ҚКЖ-ны басқару сапасының берілген параметрлерін қолдау.

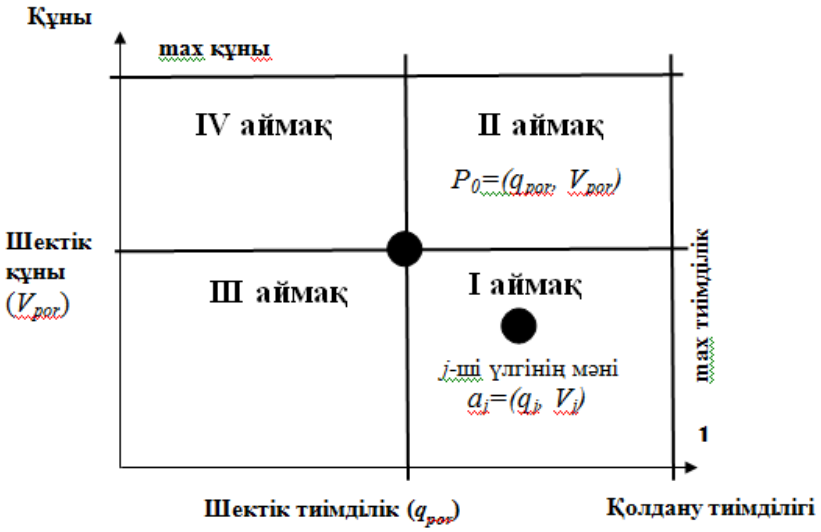
4.1.1 Жоғары оқу орнының ақпараттық білім беру ортасының қорғалуын бағалау міндеттерін шешу үшін көпкритериалды дискретті оңтайландырудың жетілдірілген әдісі

ЖОО АББО-ның қорғау құралдары мен әдістерінің рационалды нұсқаларын таңдау үшін, көпкритериалды дискретті оңтайландыру міндеттерін шешу үшін жетілдірілген Эджворт-Парето әдісін пайдалану ұсынылады. Бұл міндет ЖОО

АББО-ның қорғалу дәрежесін бағалаумен байланысты. Бұл әдісті Эджворт-Парето және лексикографиялық көпкритериалды оңтайландыру әдістеріне негізделген математикалық парадигмалар жиынтығын пайдалану арқылы жетілдіруге болады [87-89].

Диссертацияның осы бөлімінде ұсынылған аралас әдіс, қажет болған жағдайда Парето-оңтайлы шешімдер облысын кеңейтуге мүмкіндік береді. Бұл ретте ЖОО АББО-ны қорғау үшін критерийлердің маңыздылығы, сондай-ақ еселік нұсқаларды табу процедурасы ескеріледі. Ұсынылған тәсілде екі критерий қолданылады: құн критерийі және қолдану тиімділігінің критерийі. «Қолдану тиімділігі» критерийі, «құны» критерийіне қарағанда неғұрлым артықшылығы бар деген болжам жасалған. Қолданылатын критерийлердің сәйкес сандық салмақты коэффициенттері болады және олардың қосындысы барлық жағдайларда бірге тең.

Мәселені шешу процесінде қолданылатын, оңтайлылық аймақтардың схемалық көрінісі (сурет 27). Басымдық нөмірі қарастырылатын аймаққа сәйкес келеді. I аймақта оңтайлы шешімді табу жаһандық оптимум болады. Барлық басқа аймақтарда - жергілікті оптимум. II облыс ЖОО АББО-ны қорғау құралдарының құны бойынша оңтайлылық тұрғысынан оңтайлы емес (демек, ең қымбат тұратын құрылғыларды таңдау, рационалды стратегия емес). III облыс «қолдану тиімділігі» критерийі бойынша оңтайлы емес. IV облыс бірден екі критерийі бойынша оңтайлы емес.



Сурет 27 – Оңтайлы аймақтардың схемалық көрінісі

Зерттеу нысандары (ЗН) үшін ең көп еселі шешімдерді табу (қарастырылып отырған аймақтарда) моделі ұсынылған. Еселік шешімдер ЖОО АББО үшін техникалық күзет құралдарының (бұдан әрі-ТКҚ) және ақпаратты қорғау

құралдарының (бұдан әрі АҚҚ) іріктелетін нұсқалары үшін «қолдану тиімділігі» қасиетін сипаттайды. Диссертациялық зерттеуде еселі шешімдер ретінде құрылымы бойынша әртүрлі, бірақ бірдей сандық мәні бар ЗН алынған. Бұл мәндер бірдей техникалық сипаттамаларды (ТС) бейнелейді. Немесе бір критерий бойынша бірдей сандық шамаларға ие болады. Егер, кем дегенде бір ЗН үшін еселі мәндер табылса, онда осы нысандар үшін екінші критерий бойынша олардың сандық мәндеріне салыстыру жүргізіледі. Бұл ретте «құн» критерийі бойынша ең аз мәні бар нысан таңдалады. Бұл ЗН оңтайлы нұсқалар тізіміне енгізіледі, ал басқасы (буфердегі) оңтайлы шешімдер тізімінен шығарылады.

Табылған екі ЗН үшін сәйкес критерилері бойынша мәндері тең болатын жағдай болуы мүмкін. Онда осы екі нысан да шешімдер тізіміне қосылады.

Диссертацияның 4-тарауының шеңберінде жүргізілетін зерттеулер барысында әрбір аймақ үшін қарастырылатын аймақта мүмкін болатын үш нәтиженің бірі алынады:

- оңтайлы ЗН жоқ;
- бір оңтайлы ЗН бар;
- кемінде екі оңтайлы ЗН бар.

АҚЖ-ны таңдау есептерінде «Эджворта-Парето» әдісі векторлық оңтайландырудың есептеу әдістеріне жататын негізгі және қарапайым математикалық әдістердің бірі [81-85]. Бұл әдіс N критерий бойынша қарастырылып отырған зерттеу нысандарының жиынынан (S) оңтайлы зерттеу нысанын көпкритериалды таңдау есептерінің класына жатады.

Әрбір зерттеу нысаны О матрицасының j-ші баған - вектор ретінде көрсетілген (4.1).

$$O(\bar{o}_{ij}) = \begin{pmatrix} \bar{o}_{11} & \bar{o}_{12} & \dots & \bar{o}_{1j} & \dots & \bar{o}_{1S} \\ \bar{o}_{21} & \bar{o}_{22} & \dots & \bar{o}_{21} & \dots & \bar{o}_{2S} \\ & & \dots\dots\dots\dots\dots & & & \\ \bar{o}_{i1} & \bar{o}_{i2} & \dots & \bar{o}_{ij} & \dots & \bar{o}_{iS} \\ & & \dots\dots\dots\dots\dots & & & \\ \bar{o}_{N1} & \bar{o}_{N2} & \dots & \bar{o}_{Nj} & \dots & \bar{o}_{NS} \end{pmatrix} . (4.1)$$

Осы векторлар элементтерінің мәндері сәйкес критерийлердің қасиеттерін сипаттайды. Әрбір О матрицасының жол - вектор элементтерінің мәні сандық мәндермен берілген, вектор ретінде қарастырылған. Жол –векторлардың саны (N) критерийлердің санына немесе ТС санына тең.

О матрицасының і жолы үшін мына вектор берілген:

$$\overline{Q}_{\text{i}} = (\overline{o}_{\text{i1}}, \overline{o}_{\text{i2}}, ..., \overline{o}_{\text{ij}}, ..., \overline{o}_{\text{iS}}),\ S = \dim(\overline{Q_i}) \mid \forall i \in \overline{1, N}\ . \qquad (4.2)$$

$\overline{o}_{\text{ij}} \mid i = \overline{1, N};\ j = \overline{1, S}$ элемент j-ші зерттелетін нысанның *i*-ші критерийі бойынша қасиеті болып табылатын сандық мәнді анықтайды. *i*-ші критерий элементтері өлшемнің реттік шкаласымен тіркелген, тек сандық немесе тек сапалық мәндер болуы мүмкін. Әрбір критерий үшін сандық мәндері математикалық әдістердің көмегімен алынады [86,87].

Қосымша вектор енгізу ұсынылады: $\overline{P}_0 = (p_1, p_2, ..., p_{\text{i}}, ..., p_{\text{N}})$, мұндағы $N = \dim(\overline{P}_0)$.

$\overline{P}_0$ векторының элементтерінің мәндерін таңдау процесінде оңтайлы және оңтайлы емес аймақтардың арасындағы шекараны сипаттайды. $\overline{P}_0$ вектордың сандық мәнін шешім қабылдауға жауапты тұлға (ШҚЖТ) белгілейді. Альтернатива ретінде, $\overline{P}_0$ вектор математикалық әдістермен есептеледі.

Әрбір критерий өзініне сәйкес салмаққа ие болған жағдайда, қарастырылып отырған әдіс Подиновскийдің лексикографиялық әдісі деп аталады [87,89]. Сәйкес ЗН үшін баған – вектордың мәні қарастырылатын критерий бойынша қарастырылатын үлгі оңтайлы болатынын немесе болмайтынын анықтауға мүмкіндік береді. Қарастырылып отырған векторлық оңтайландыру әдісін қолданған жағдайда, қарастырылатын критерий бойынша бір немесе бірнеше ЗН оңтайлы емес болып табылатын жағдайлар болуы мүмкін. Бұл жағдайда ШҚЖТ осы ЗН-ді оңтайлы тізімге қоса алады. Сонда оңтайлы нысандар тізімінде барлық критерий бойынша бірдей мәндері бар бірнеше ЗН болады. Бұл жағдайда ШҚЖТ сарапшыларға осы ЗН ең қолайлысын таңдау мақсатында өз бетімен немесе ШҚҚЖ көмегімен қарастыруын сұрайды.

4.1.2 «Тиімділік-құн» критерийін қолдану кезінде жоғары оқу орнының ақпаратты білім беру ортасында қолжетімділік пен киберқауіпсіздігін басқару, бақылау жүйесінің компоненттерін таңдау алгоритмі

Алгоритм 4.1. тарауда сипатталған әдісті жүзеге асырады. Алгоритмнің блок-схемасы көрсетілген (сурет 28). Ыңғайлы болу үшін алгоритм кезеңдерге бөлінген:

1 кезең. Алгоритмді орындау, зерттеу нысаны (ЗН) элементтерінің саны - *S* бойынша бастапқы мәліметтерді енгізуден басталады. Мәліметтер массиві екі вектор түрінде $\left\{\overline{Q}, \overline{V}\right\}$ беріледі.

2 кезең. Оңтайлы аймақтың шегі болып табылатын $\{q_{\text{por}},\ V_{\text{por}}\}$ екі мәні енгізіледі. Осылайша $\overline{P}_0$ векторы беріледі.

3 кезең. Критерийлердің маңыздылығын есепке алу үшін олардың салмақ коэффициенттерінің мәндері беріледі. Сонымен бірге,

$\{\alpha_{1*}\overline{Q}, \alpha_{2*}\overline{V}, \alpha_{1*}q_{\text{por}}, \alpha_{2*}V_{\text{por}}\}$ формуласы бойынша $\{\overline{Q}, \overline{V}, \overline{P}_0\}$ векторлардың элементтерін қайта есептеу жүргізіледі, мұндағы $\{\alpha_1, \alpha_2\}$- салмақ коэффициенттерінің мәндері, [88] бойынша қабылданған.

4 кезең. Басқару I блокқа – I аймақтан шешімді іздеу блогына беріледі (сурет 29). I блокта $\overline{Q}$ векторының q_{j} элементіне іздеу жүргізіледі. q_{j} мәні максималды және берілген q_{por} шегінің шамасынан асатын элемент болу керек. Егер мұндай элемент табылған болса, онда екінші критерий бойынша оңтайлылыққа тексеріледі.

5 кезең. q_{i} мен бір позицияда тұрған $\overline{V}$ векторының v_{j} элеметтінің мәнін V_{por} – тың мәнімен салыстырады. Егер ізделетін мән V_{por} аспаса, онда бұл элемент оңтайлы үлгілердің тізіміне енгізіледі. Егер v_{j} мәні V_{por} асса, онда бұл элемент тізімнен шығарылады және бағдарлама I блоктың басына қайтарылады.

6 кезең. Келесі элементті тізімде қалған элементтердің ішінен іздейді. Алгоритмде «қолдану тиімділігі» критерийі бойынша еселі мәндердің масималды санының бар болуын тексеру қарастырылған. $\overline{Q}$ вектордан еселі мәндері бар элементтер табылған кезде, ал V критериі бойынша I аймақты қанағаттандыратын элементтер табылған кезде, осы элементтердің мәндерін $\overline{V}$ вектор бойынша салыстыру жүргізіледі. «Құны» критерийі бойынша шамасы аз болатын үлгі таңдалады. I блоктағы алгоритмнің нәтижесі оңтайлы техникалық шешімді таңдау (немесе таңдаудың болмауы). Осыдан кейін, сарапшылар таңдалған шешімді қабылдау туралы сұрақты қарастырады. Нәтиже оң болған жағдайда, осы шешім бекітіледі және есептеу процесі аяқталады. Ал техникалық шешім қабылданбаған жағдайда, осы шешім қаралатын шешімдер тізімінен алынып тасталады және басқару қайтадан I блокқа беріледі.

Егер I блокта есептеу процесін орындау барысында оңтайлы шешім жоқ болса немесе ол шешім қабылдау кезінде қабылданбаса, онда басқарудың II блокқа өтуі қарастырылған. II блокта «қолдану тиімділігі» (II аймақ) критерийі бойынша оңтайлы болған кезде «құн» критерийі бойынша оңтайлы шешімді іздеу процесі жүреді (сурет 30).

7 кезең. Алдымен q_{por} шектік мәнінен асатын, $\overline{Q}$ векторының барлық элементтері табылады. Таңдалған элементтердің индекстері уақытша тізімге енгізіледі, атап айтқанда мына өрнекті қанағаттандырады:

$$\{q_{k_1}, q_{k_2}, ..., q_{k_g}, ..., q_{k_f}\} \mid q_i \geq q_{por};\ k_g = i,\ \forall i = \overline{1, S}. \qquad (4.3)$$

8 кезең. Бұдан әрі, тізімнен құн критерийінің мәні V_{por} - шекті мәніне жақын болатын элементтерді іздеу жүзеге асырылады және мына өрнекті қанағаттандырады:

$$v = v_i = \min\{v_{k_1}, v_{k_2}, ..., v_{k_g}, ..., v_{k_f}\} \mid k_g = i,\ \forall i = \overline{1, S}. \qquad (4.4)$$

Егер мұндай элементтер табылмаса, онда басқару II блоктан шығады. Егер іздеу сәтті аяқталса (элементтер табылса), онда ең жоғары тиімділігі және ең төмен құны бар элементті іздейді. II блокта, сондай-ақ, еселі мәндердің неғұрлым масималды санын іздеу процесі қарастырылған. Егер мұндай мәндер жоқ болса, онда осы аймақтан шешімдерді іздеу тоқтатылады. II аймағы іздеу нәтижелерін қабылдауға ұсынады.

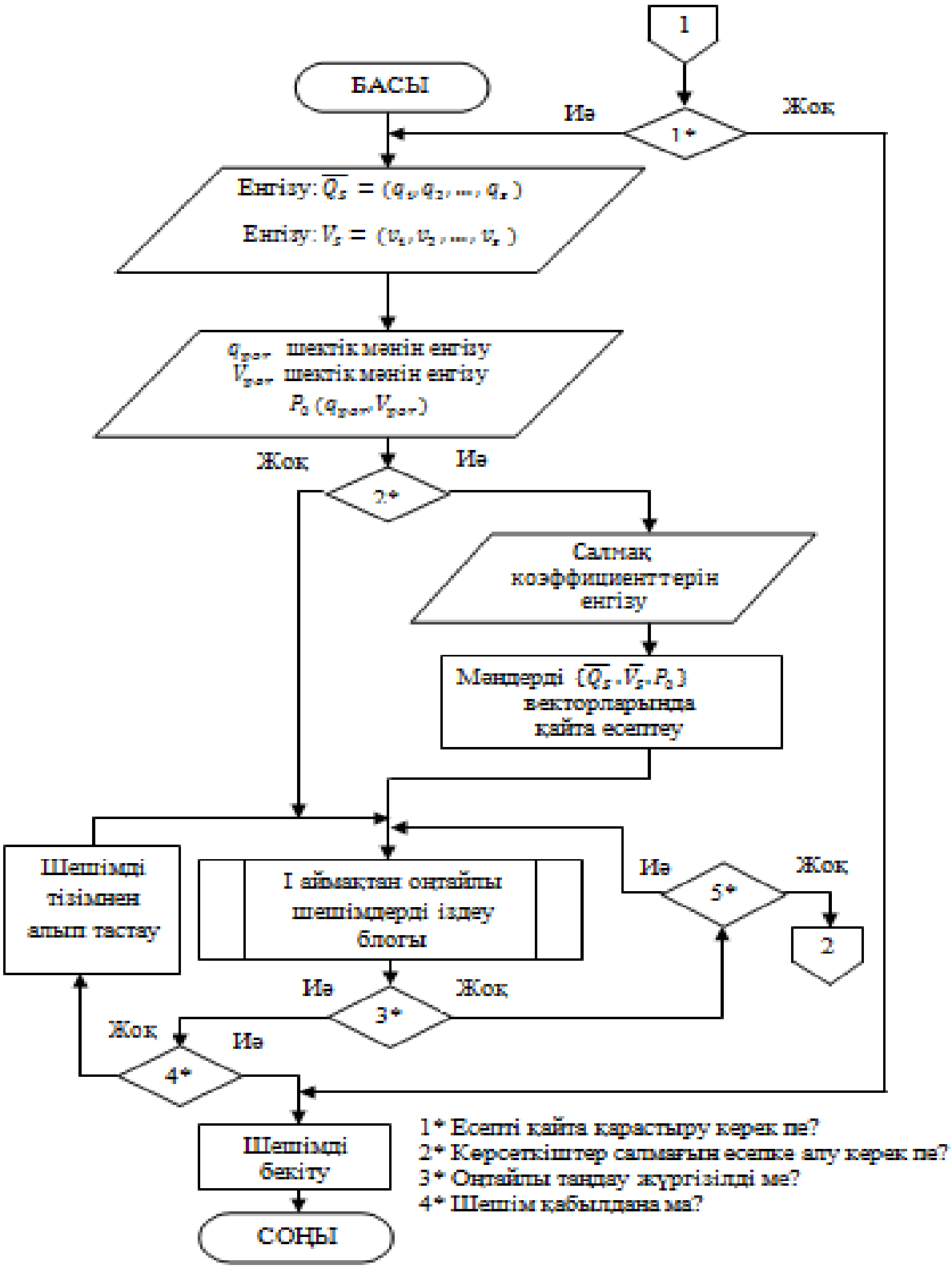
9 кезең. Егер I және II аймақтардан іздеу нәтижелері қанағаттандырмаса, онда алгоритм III және IV аймақтардан оңтайлы шешімдерге жақын шешімдерді іздестіруді көздейді.

10 кезең. III блокта III аймақтан оңтайлы шешімді іздеу процесі жүзеге асырылады. Басында V_{por} шекті мәнінен аспайтын $\overline{V}$ векторының элементтерінің барлық мәндерін табу процесі жүреді. Таңдалған элементтердің индекстері уақытша тізімге енгізіледі. Егер мұндай мәндер жоқ болса, онда басқару III блоктан шығады. Содан кейін, индексі уақытша тізімге енгізілген, мәні максималды болатын элементті $\overline{Q}$ вектордан таңдайды. Алгоритм "тиімділік" критерийі бойынша еселі мәндердің неғұрлым максималды санын табуды қарастырады. Еселі мәндер болмаған жағдайда, басқару III блоктан шығады. Егер еселі мәндер табылса, онда "құн" критерийі бойынша ең төменгі мәнге ие болатын элементті іздеу жүзеге асырылады. Егер табылған құнның мәні шектеуден аспаса, онда элемент ұсынылатын нұсқалар тізіміне енгізіледі.

Егер табылған құнның мәні шегінен асып кетсе, онда басқару III блоктан шығу жүзеге асырылады. II аймағы табылған нәтижелерді қабылдауға ұсынады.

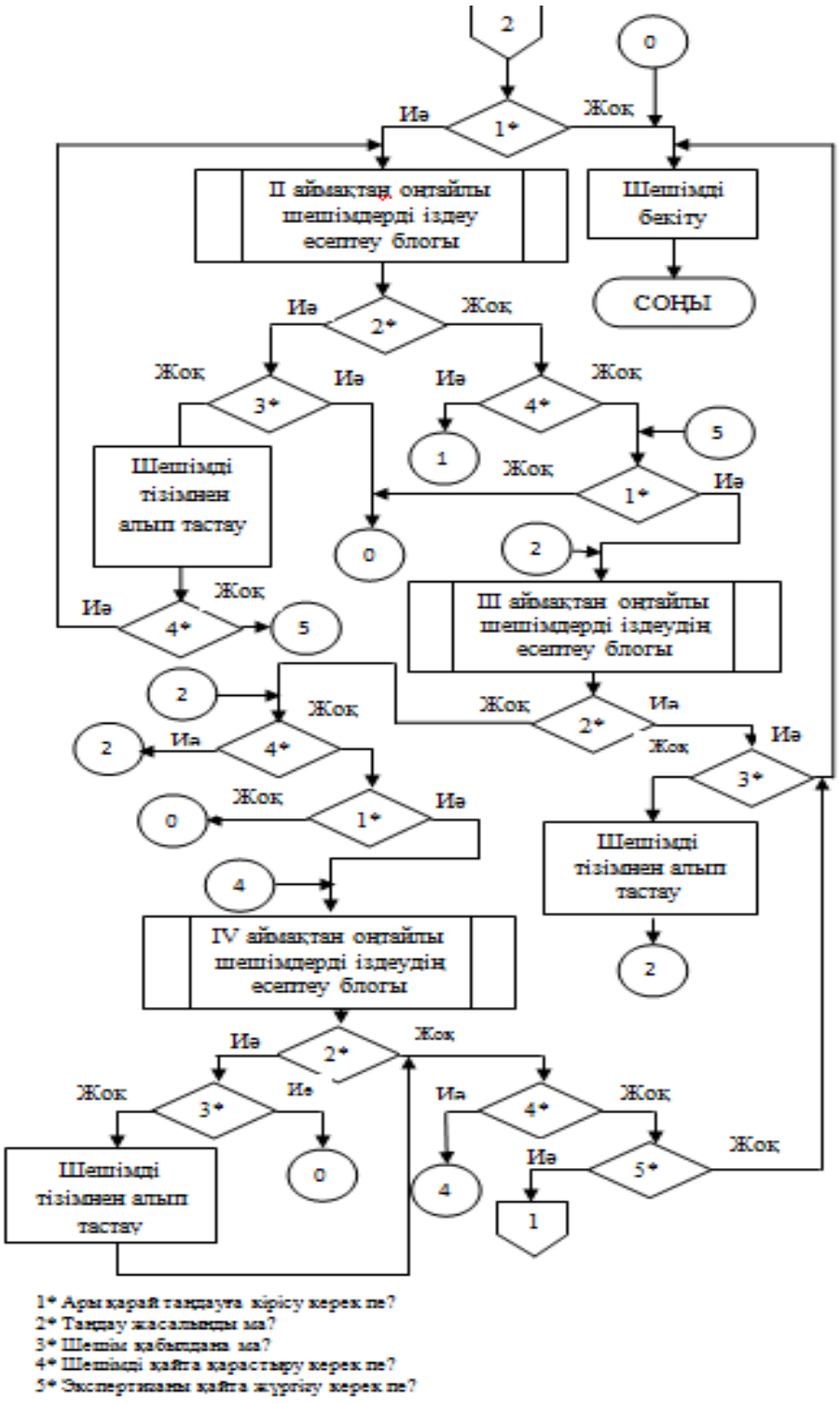
11 кезең. I, II, III аймақтарда шешімнің оңтайлы нұсқалары болмаған жағдайда алгоритм ғаламдық оңтайлы емес IV аймағында шешімнің нұсқаларын іздеуді көздейді. Бұл IV есептеу блогында жүзеге асырылады. q_{opt}, және v_{opt} ең жақын мәндерді табу үшін, іздеу алғашқыда Q критерийі бойынша, содан кейін V критерийі бойынша жүргізіледі.

Алгоритм ұсынылған техникалық нұсқалардың I аймақта оңтайлы шешімдер (ғаламдық оптимум) болуын қайта қарауды жүзеге асыруды көздейді. Ұсынылған нұсқаларды қабылдамаған кезде алгоритмде бір ғана критерий (қолдану тиімділігі немесе құны) бойынша оңтайлы шешімдерді, ғаламдық оңтайлы емес II немесе III және IV аймақтарда іздеуге көшу қарастырылған. Егер қайта қарау қабылданбаса немесе нұсқаларды одан әрі таңдау тоқтатылса, алгоритм оңтайлы шешімдерді іздеу процесі туралы есебін техникалық жүйелердің ұсынған нұсқаларынан қалыптастырады.



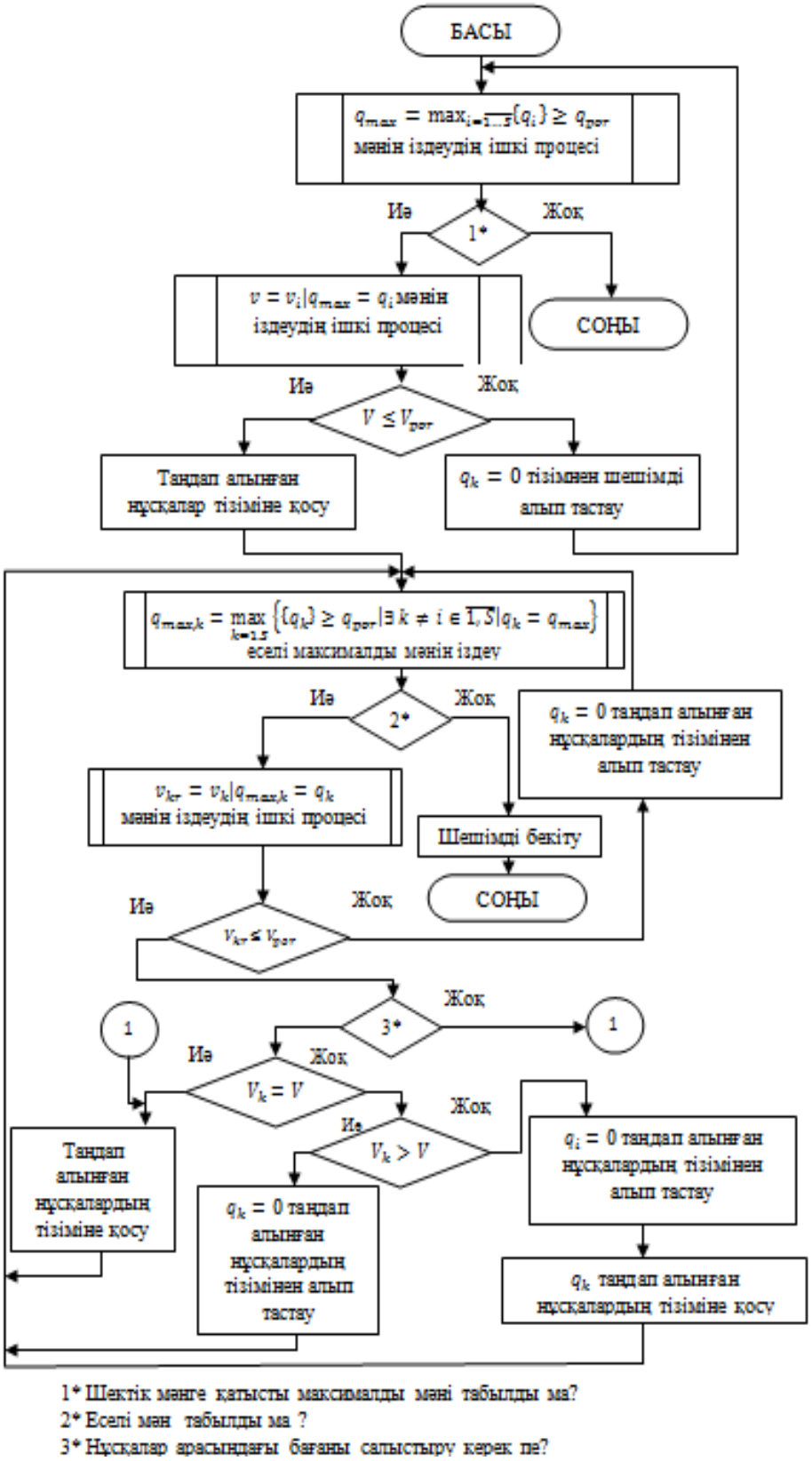
а) алгоритмнің басы

Сурет 28- «Тиімділік - құн» критерийі бойынша қолжетімділікті басқару және бақылау жүйесін оңтайлы таңдау алгоритмі (жалғасы), бет 1

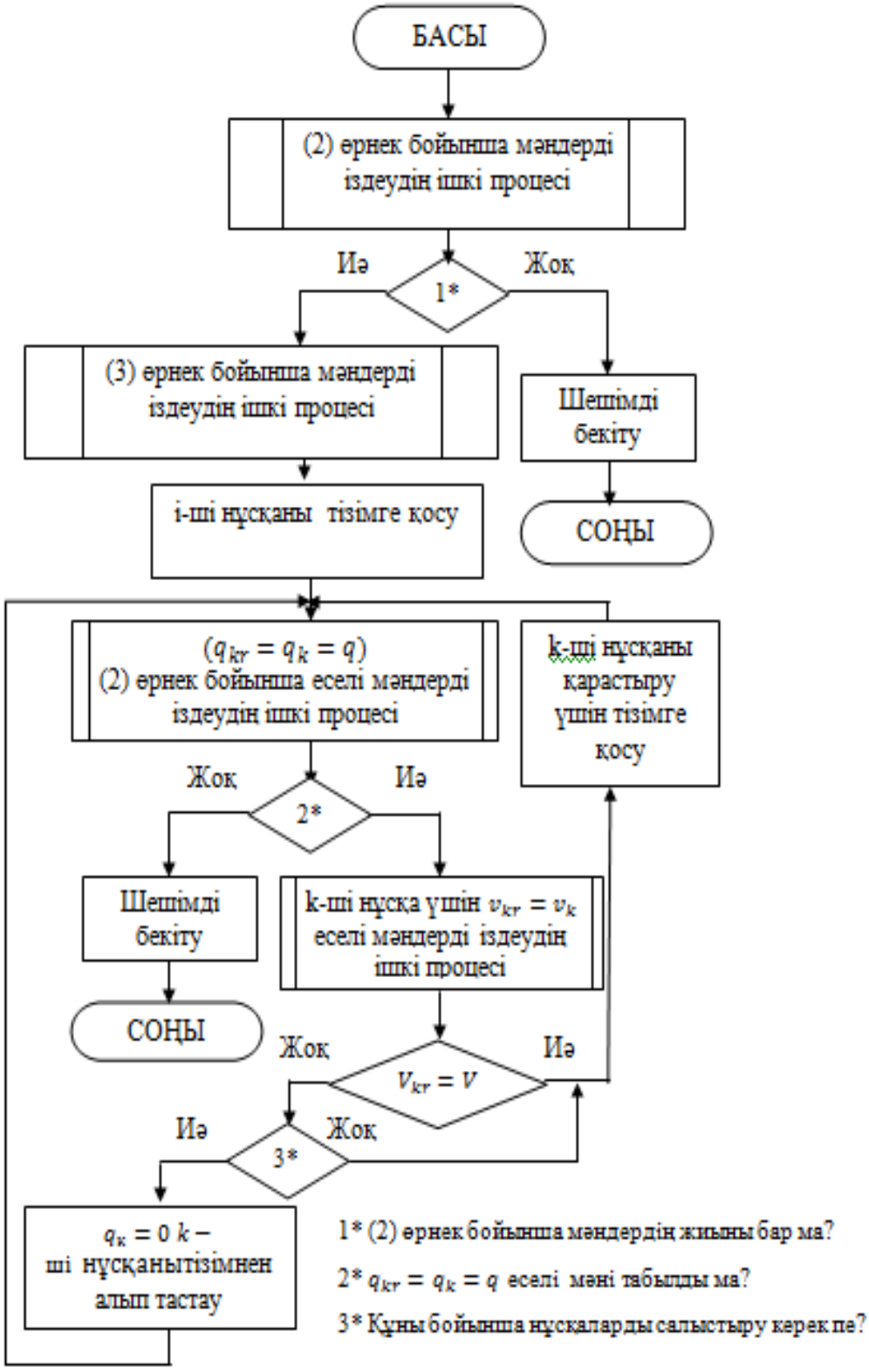


б) алгоритмнің соңы

Сурет 28- «Тиімділік - құн» критерийі бойынша қолжетімділікті басқару және бақылау жүйесін оңтайлы таңдау алгоритмі (жалғасы), бет 2



Сурет 29 - (I) аймақта оңтайлы шешім табудың алгоритмінің блок-схемасы (I блок алгоритмі)



Сурет 30 - (II) аймақта оңтайлы шешім табудың алгоритмінің блок-схемасы (II блок алгоритмі)

Ұсынылған әдіс және ЖОО АББО үшін ТКҚ және АҚЖ таңдау кезінде оңтайлы шешімді іздеу алгоритмінің жоғарыда сипатталған кезеңдері, диссертацияның келесі бөлімінде сипатталған «DSS ШҚҚЖ модулі (АҚЖ таңдау үшін Парето әдісі)» компьютерлік бағдарламасында жүзеге асырылды. «DSS ШҚҚЖ модулі (АҚЖ таңдау үшін Парето әдісі)» дербес бағдарламалық өнім ретінде, сонымен қатар, бұрын диссертациялық жұмыстың 2 және 3 тарауларында баяндалған модельдерден тұратын ЖОО АББО киберқауіпсіздігін инвестициялау бойынша стратегиялардың рационалды нұсқаларын таңдау бойынша шешімдерді қабылдауды қолдау жүйесінің модулі ретінде де қолданылуы мүмкін.

Әлбетте, ЖОО АББО-ға кіріктірілген қорғауды жағдайға байланысты басқару аясындағы кез келген іс-шаралар қаржыландыруды талап етеді. Сондықтан диссертациялық жұмыстың келесі бөлімінде зерттеу шеңберінде құрылған, ЖОО АББО-ның КҚ және АҚ жүйелерін құру немесе жетілдіру үшін рационалды қаржы стратегияны табу бойынша міндеттерді шешуді автоматтандыруға мүмкіндік беретін бағдарламалық өнімдер сипатталған.

4.2 Технологияны және бағдарламалау тілін таңдауды негіздеу

Сапалы бағдарламалық өнімдерді құрудың қолданыстағы әдістері және сәйкес ақпараттық технологиялары, қолданбалы бағдарламалық қамсыздандыруды (ҚБҚ) қолданатын немесе оны өмірлік циклындағы барлық кезеңдерінде сүйемелдейтін, кез - келген қолданушыға немесе программистке түсінікті болатындай құруға мүмкіндік береді.

Нақты есеп үшін бағдарламалау тілін таңдау, жоба сипаты және ҚБҚ талаптарына байланысты алдын ала анықталған.

ЖОО АББО-дағы АҚ және КҚ бойынша іс-шараларды және құралдарды қаржыландырудың рационалды стратегиясын таңдау үшін құрылатын бағдарламалық өнімге қойылатын талаптарды төмендегідей тұжырымдауға болады:

1) Нәтижелердің дұрыстығы (корректность). Бағдарлама қолданушы енгізетін кез -келген мәлеметтер үшін дұрыс нәтижелер беруі тиіс. (Бастапқы мәліметтердің рұқсат етілген диапазондары алдын ала келісіледі).

2) Қолданылатын алгоритмдердің тиімділігі. Құрылған ҚБҚ дербес компьютердегі ресурстарды аз қолданған жағдайдың өзінде, тиімді нәтижелер беруі тиіс.

3) Сенімділік. Қолданушы құрылған бағдарламалық өнімнің көмегімен алынған нәтижелерге сенуі тиіс. ҚБҚ-ны қолданудың кез келген шарттары кезінде, нәтиже ДК жұмысында болуы мүмкін өрескел қателіктерге әкелмеуі керек.

4) Әмбебаптылық. Құрылған ҚБҚ енгізілетін мәліметтердің кең диапазонына есептелген болуы керек.

5) Функционалдығы. Құрылған ҚБҚ қолданушының барлық негізгі қажеттіліктерін қамтамасыз етуі және нақты есепті шешу үшін ҚБҚ-ны жүктеу кезінде қосымша кітапхана файлдарының көмегінсіз жұмыс істеуі керек.

6) Қолдану кезіндегі ыңғайлылығы. Құрылған ҚБҚ қолданушының игеруі мен пайдалануына ыңғайлы болуы тиіс. Бұл ретте терезе интерфейсі интуитивті түсінікті болуы керек.

7) Стандарттау. Құрылған ҚБҚ-да мәліметтерді енгізу мен шығаруды басқарудың типтік құралдары (интерфейс) болуы тиіс.

8) Тасмалдануы. Құрылған ҚБҚ баптаулардағы ең аз өзгерістермен әртүрлі ЖОО АББО-ның стратегияларын бағалау үшін, әр түрлі ДК-дан мәліметтерді тасымалдау мүмкіндігін қамтамасыз етуі тиіс.

9) Кодтың оқылуы. Бағдарлама коды жобамен жұмысты жалғастыра алатын басқа программистер қабылдай алатындай және түсінетіндей, барынша оқылатын болуы тиіс.

10) Модификациялау мүмкіндіктері. Құрылған ҚБҚ жаңа функционалмен өзгеру және толықтырылу мүмкіндіктерін қарастыруы тиіс.

11) Ілеспе құжаттаманың болуы. Құрылған ҚБҚ оны қолдану жөніндегі нұсқаулықпен жабдықталуы тиіс.

ЖОО АББО-ның АҚ-ны және КҚ-ны қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау бойынша ҚБҚ жобасы NET. Framework 3.5. ортасында C # 3.0 тілінде жүзеге асырылған.

Бағдарламалау тілін таңдау кезінде екі негізгі есеп қойылды - құру жылдамдығы және бағдарламаны құрастыру кезеңінде қателер туралы білу мүмкіндігі. Дәл осындай талаптар жасалды, себебі техникалық жүзеге асыру, бірінші кезекте, алдыңғы тарауларда құрылған теориялық бөлімді тексеру, демек, ең аз қателік санымен тәсілді барынша толығымен жүзеге асыру мақсаты бар. Сонымен қатар, табылған нәтижелер теориялық негізделу үшін кері кері байланыс беретіндіктен, біз есептің қойылымында немесе верификацияланған алгоритмдер үшін, тиісті өзгерістер жасау кезінде бағдарламалық кодты жылдам өзгерту мүмкіндігіне ие болуымыз керек.

Біз талаптардың арасында компиляция кезеңінде қателерді анықтау талабын қойғандықтан, Python сияқты динамикалық тілдерден бас тарттық. Python - да қарапайым бағдарламаларды жазу салыстырмалы түрде тез құрастырылады, бірақ бағдарламаны қолдау және модификациялау кезінде қиындықтар туындайды. Сондықтан, үміткерлер тізімін C++, Java, C # сияқты тілдерге дейін қысқарттық.

Java тілі C ++ тілінің синтаксисін нығайту трендінің нәтижесі ретінде пайда болғанын ескереміз. Java жасаушылары C++ тіліндегі бағдарламалық өнімдердің жазылу тәжірибесіне негізделе отырып, сәтсіз шешімдерден құтылуға тырысты. Мысалы, Java-да операторларды қайта анықтау немесе сәйкес келмейтін типтерді автоматты түрде келтіру қарастырылмаған. Java интерфейстері түсіну үшін

қарапайым және анық. Бірақ C++ тілінен Java тілі ҚБҚ парадигмасының барлық артықшылықтарын мұра етті.

Жалпы C # тілінің синтаксисі C ++ және Java алгоритмдік тілдерінің синтаксисінің барлық артықшылықтарын алған.

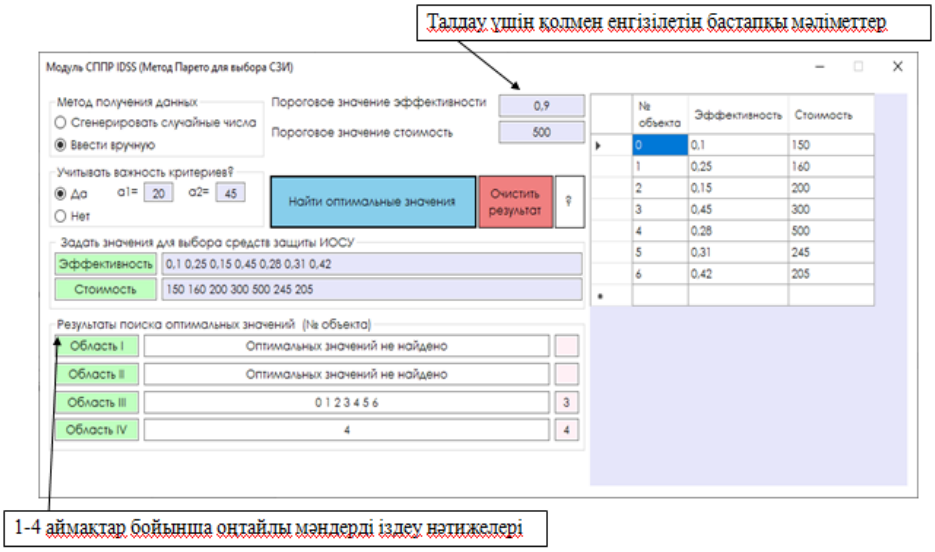
Алайда, C # тілі үшін Java-да қарастырылмаған C++ тілінің кейбір мүмкіндіктерін көшіру туралы шешім қабылданды. Мысалы, мұндай мүмкіндіктерге мыналарды жатқызуға болады: таңбасыз типтерді пайдалану, операцияларды қайта анықтау мүмкіндігі, сілтеме бойынша әдістерге параметрлерді беру, параметрлерінің саны өзгеріп отыратын әдістерді пайдалану және т.б.

Сондықтан, C # тілі бір уақытта функционалдық және нысанға-бағытталған тәсілдерді қолдайды, сондықтан ҚБҚ-ны құру үшін базалық тіл ретінде осы тілді таңдадық. Жобалау ортасы ретінде VisualStuduo 2017 ортасы таңдалды.

4.3. «Шешімдерді қабылдауды қолдау жүйесі (ШҚҚЖ) модулі (ақпаратты қорғау жүйесін таңдау үшін Парето әдісі)» - бағдарламалық өнімнің сипаттамасы

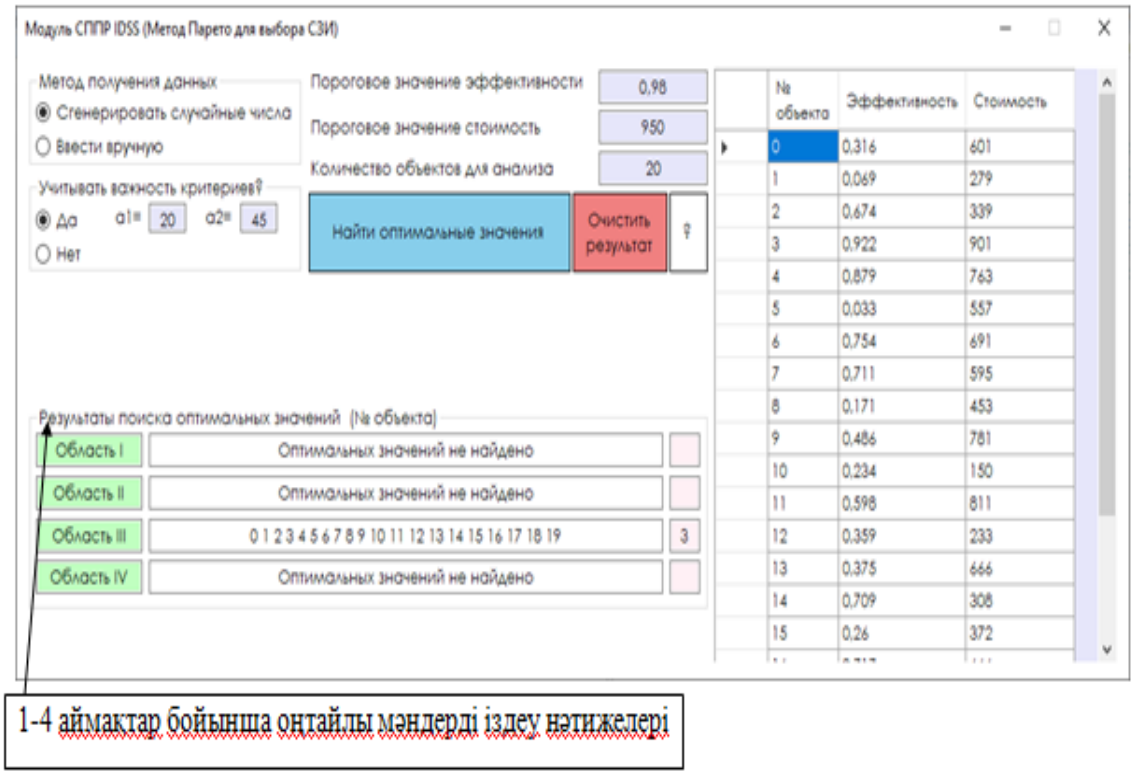
«ШҚҚЖ (DSS) (АҚЖ-ны таңдау үшін Парето әдісі)» модулі бағдарламасының (бағдарламалық өнімнің) жалпы түрі көрсетілген (сурет 31).

Бұл ШҚҚЖ модулінде кез келген қолданушыға интуитивті түсінікті классикалық терезе интерфейсі бар. Енгізілген параметрлерді бақылаудың дамыған жүйесі модельдеу және кейінгі талдау үшін бастапқы параметрлердің дұрыс енгізілуіне кепілдік береді.



а) ЖОО АББО-ның ТКҚ және АҚЖ компоненттерін таңдау үшін бастапқы мәліметтерді қолмен енгізу

Сурет 31- «ШҚҚЖ (АҚЖ таңдау үшін Парето әдісі)» модулінің графикалық интерфейсі, бет 1

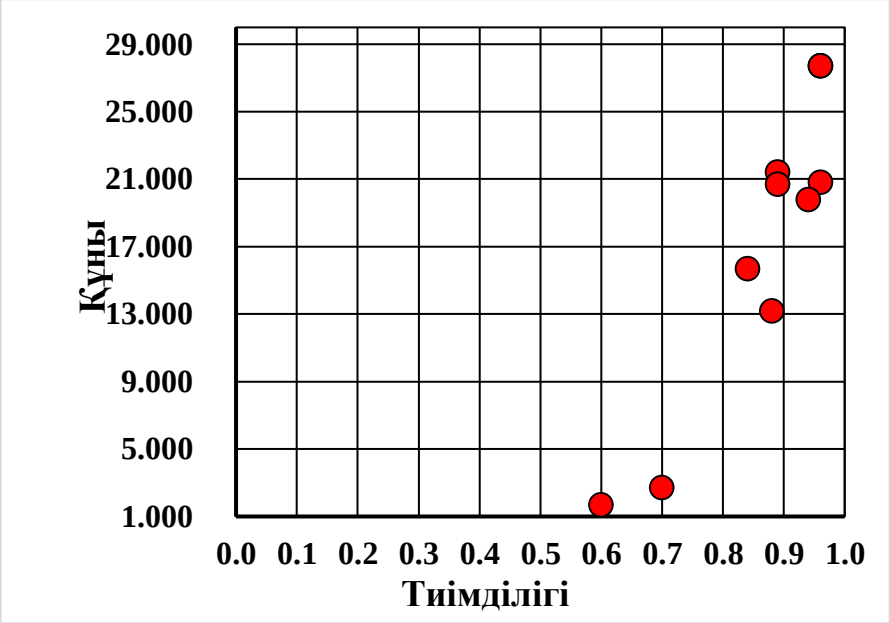


б) ЖОО АББО-ның ТКҚ және АҚЖ компоненттерін талдау үшін параметрлердің автоматты генерациясы

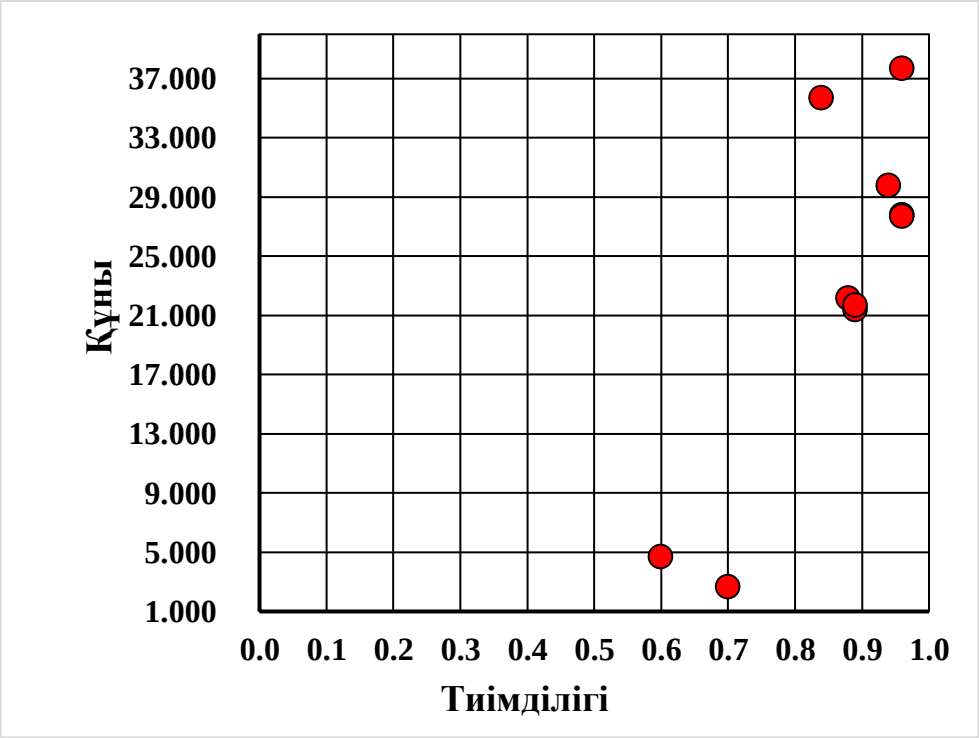
Сурет 31- «ШҚҚЖ (АҚЖ таңдау үшін Парето әдісі)» модулінің графикалық интерфейсі, бет 2

«ШҚҚЖ (АҚЖ-ны таңдау үшін Парето әдісі)» модулі бағдарламасының жұмыс қабілеттілігі есептеу эксперименттері барысында тексерілді (сурет 32,33). Бастапқы мәліметтер ретінде, [93-95] бағдарлама мәліметтері бойынша генерацияланған параметрлер мәндері қабылданды. «ШҚҚЖ (АҚЖ-ны таңдау үшін Парето әдісі)» модулі бағдарламасының жұмысын талдау барысында ЖОО АББО үшін ТКҚ және АҚЖ ұсынған нұсқалар арасында оңтайлы шешімді іздеу алгоритмінің дұрыс (корректно) орындалуы қадағаланды.

Генерация процесінде ЖОО АББО- ның ТКҚ үшін (сурет 32) және АҚЖ үшін (сурет 33) нүктелік графика түрінде берілген екі өлшемді массивтер алынды.



Сурет 32 - ЖОО АББО үшін ТКҚ –ның оңтайлы үлгілерін іздеудің кеңейтілген аймағы



Сурет 33- ЖОО АББО-ның компьютерлік желі сегменті үшін АҚЖ және КҚ құралдарының оңтайлы үлгілерін іздеудің кеңейтілген аймағы

Қызыл нүктелер –қарастырылатын ТКҚ үлгілері үшін тиімділік пен құн мәндерінің координаттары (сурет 32). Атап айтқанда, қызыл нүктелер – ЖОО АББО үшін ақпаратты қорғау және киберқауіпсіздік құралдарының

қарастырылатын үлгілері үшін тиімділік пен құн мәндерінің координаттары (сурет 33).

ТКҚ және ақпаратты қорғау, киберқауіпсіздік құралдары үшін қорғау нысаны ретінде компьютерлік желінің немесе жергілікті желінің сегменті қарастырылды. Құн параметрлері шартты ақша бірлігінде қарастырылады. Графикте көрсетілген нәтижелер, ұсынылған әдіс және «тиімділік–құнкритерийі» бойынша оңтайлы шешімдерді іздеудің кеңейтілген аймағы болады.

Бағдарлама мен алгоритмді тестілеу барысында алынған нәтижелердің дұрыстығы (корректность) анықталды. Нақты ЖОО АББО үшін зерттеу нәтижелерін [93-95] енгізу кезінде, ұсынылған шешімдер ЖОО АББО-ның қорғалу дәрежесін арттыруға мүмкіндік беретінін көрсетті. Ұсынылған әдіс пен алгоритм ЖОО АББО үшін ТКҚ-ны жобалаудың бастапқы сатыларында техникалық тапсырманы орындауға мүмкіндік береді.

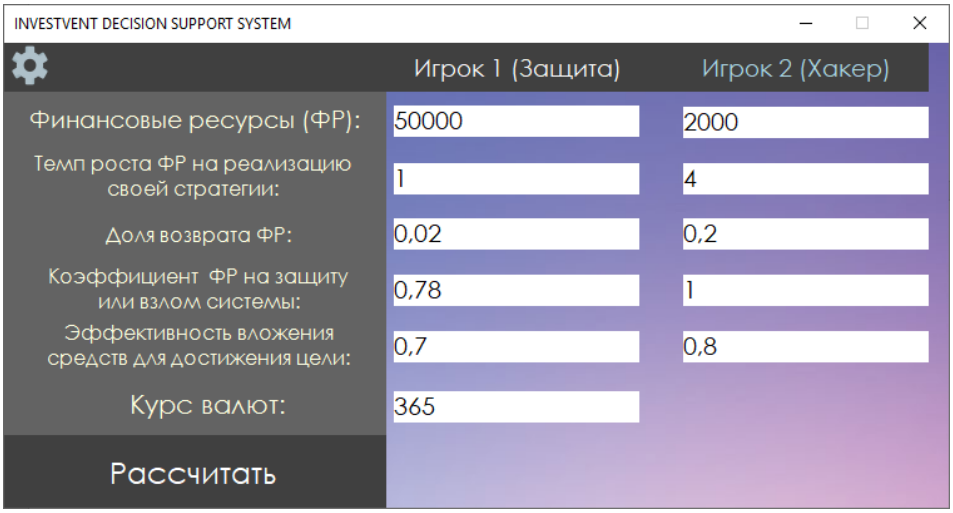
ЖОО АББО-ның қорғалуын бағалау және ТКҚ мен АҚЖ рационалды нұсқаларын таңдау есептерін шешу үшін көп критериалды оңтайландырудың жетілдірілген әдісі мен алгоритмдері ЖОО АББО-ны қорғау құралдарын таңдау кезеңіндегі шығындарды 16-19% - ке азайтуға мүмкіндік берді. Осы жетілдірілген әдіс пен алгоритмдерді зерттеу жұмыстарында [89-95] сипатталған әдістемелермен және алгоритмдермен салыстыру жүргізілді. Ұсынылған тәсіл, ұқсас шешімдермен [86,92] салыстырғанда келесі артықшылықтарға ие: көптеген төбелерден тұратын ЖОО АББО-ның қорғалу деңгейін бағалауға мүмкіндік береді; сарапшыға ТКҚ-ның және АҚЖ-ның әртүрлі кешендеріне салыстырмалы талдау жүргізуге мүмкіндік береді; нақты ЖОО-ның және ондағы АББО-дағы қызмет ету ерекшелігін және негізгі ресурстар үшін нақты қатерлерді ескереді.

Жалпы, жүргізілген зерттеулер негізінде ұсынылған әдіс пен алгоритмдердің, сондай-ақ «ШҚҚЖ (АҚЖ-ны таңдау үшін Парето әдісі)» модулі бағдарламалық өнімінің тиімділігін растауға болады. «ШҚҚЖ (АҚЖ-ны таңдау үшін Парето әдісі)» модулі бағдарламалық коды көрсетілген (Қосымша А).

4.4. «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау» ШҚҚЖ бағдарламалық өнімінің сипаттамасы

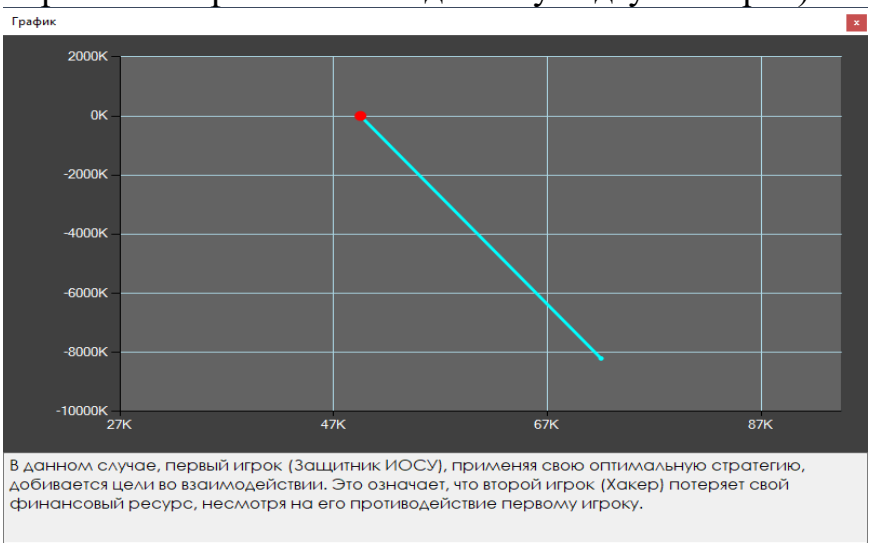
«ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» ШҚҚЖ модулінің жалпы түрі көрсетілген (сурет 34). Бағдарламаның негізгі терезелері көрсетілген (суреттер 35-40).

Бастапқы мәліметтер ретінде Украина және Қазақстан Республикасының жоғары оқу орындарының қорғалған АББО-ны құруға берілген техникалық тапсырмалар алынды.

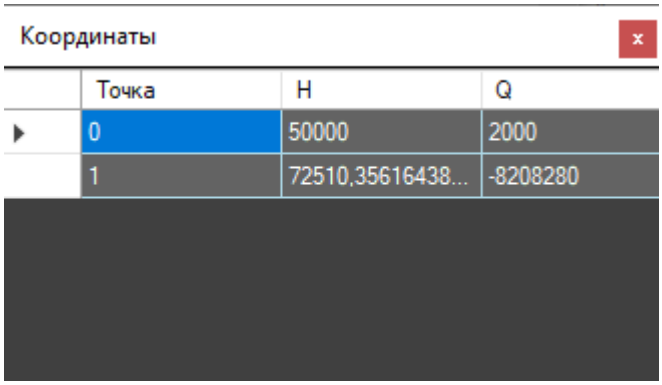


Сурет 34 - «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау» ШҚҚЖ модулінің жалпы түрі

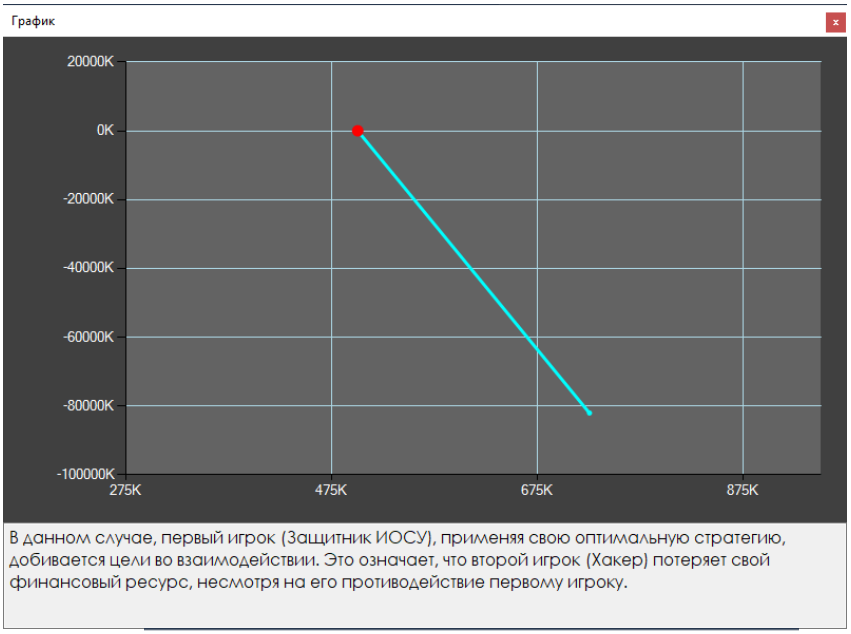
«ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» ШҚҚЖ модулін тестілеу барысында екі ойыншы (ЖОО АББО қорғаушысы – 1 –ші ойыншы және 2-ші ойыншы-хакер) динамикалық жүйені басқаратын жағдайлар қарастырылды. Эксперимент мақсаты ойыншылардың стратегиялар жиынын анықтау. Ойыншылардың стратегиялары оларды тиісті терминалдық беттерге шығаратын жағдайлар қарастырылады. Эксперимент барысында нысандарға жүйені осы немесе басқа терминалдық бетке келтіруге мүмкіндік беретін, нысандардың бастапқы күйілерінің жиыны және олардың стратегиялары табылады. Жазықтықта абсцисса осі-1 ойыншының қаржы ресурстары (ЖОО АББО қорғаушысы). Ордината осі - 2 ойыншының қаржы ресурстары (хакер немесе тұтастай алғанда шабуылдаушы тарап).

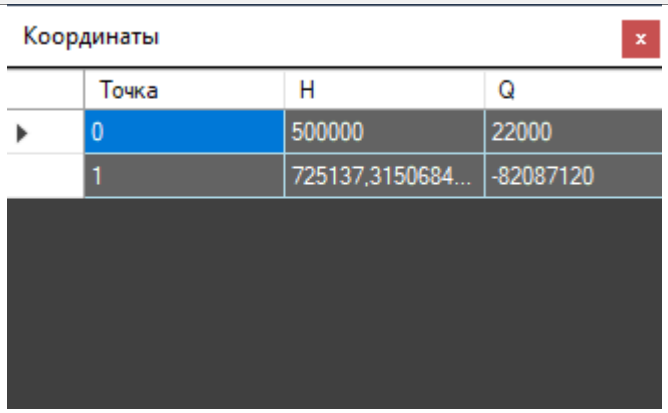


Сурет 35- ШҚҚЖ «DSS»-ның жұмыс нәтижелері (Есептеу эксперименті 1), бет 1



Сурет 35- ШҚҚЖ «DSS»-ның жұмыс нәтижелері (Есептеу эксперименті 1), бет 2



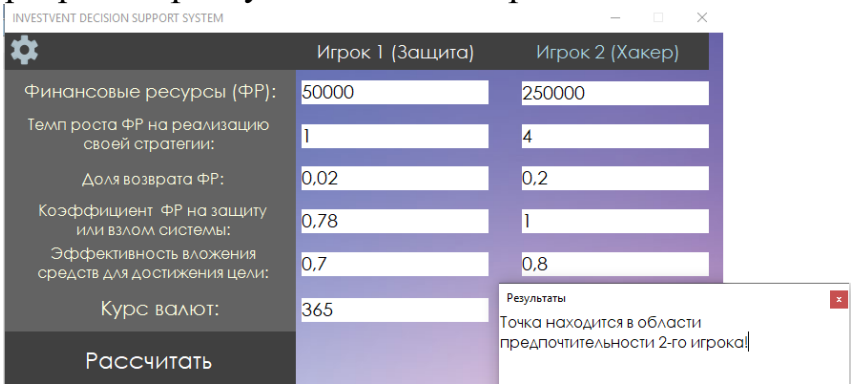


Сурет 36- ШҚҚЖ -ның жұмыс нәтижелері (Есептеу эксперименті 2)

Алынған нәтижелер 2-тарауда ұсынылған тәсілдің тиімділігін көрсетеді. Модельді және бағдарламалық өнімді тестілеу барысында алынған нәтижелердің дұрыстығы (корректность) анықталды. «ЖОО АББО киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» ШҚҚЖ модулін сынақ Украина мен Қазақстанның ЖОО АББО-ның киберқауіпсіздік саласындағы нақты инвестициялық жобалар үшін орындалды.

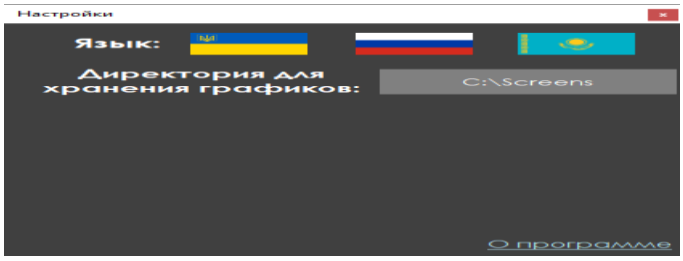
Бірінші ойыншы (ЖОО АББО қорғаушысы) бастапқы қаржы ресурстарының қатынасында артықшылығы бар жағдайды бейнелейді, атап айтқанда олар 1-ші ойыншының «қалау» аймағында орналасқан. Бұл жағдайда 1-ші ойыншы өзінің оңтайлы стратегиясын қолдана отырып, өз мақсатына жетеді, атап айтқанда жүйе күйін «өзінің» терминалдық бетіне әкеледі (суреттер 35-39).

2-ші ойыншы (хакер) бастапқы уақытта 1-ші ойыншының оңтайлы емес әрекетін пайдалана отырып, жүйенің күйін «өзінің» терминалдық бетіне «әкеледі» деген жағдайға қол жеткізеді (суреттер 37,38). Мұндай жағдайда ЖОО АББО-ның қорғаушы тараптары үшін болжам қолайсыз. Атап айтқанда ЖОО АББО-ға шабуылдаушы тараптың (ойыншы - Хакер) біліктілігі жоғары болған жағдайда, қорғау периметрлерінің бұзылу ықтималдығы үлкен болады.

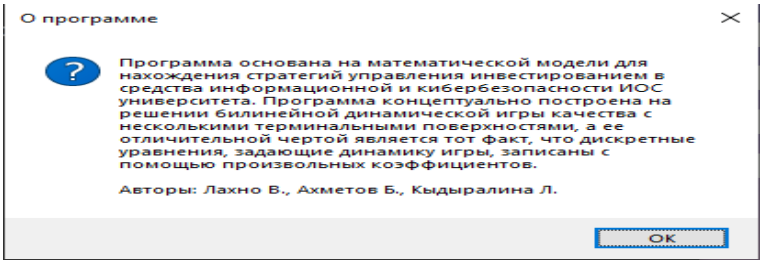


Сурет 37- ШҚҚЖ «DSS»-ның жұмыс нәтижелері (Есептеу эксперименті 3)

Сурет 38 - ШҚҚЖ «DSS»-ның жұмыс нәтижелері (Есептеу эксперименті 4)



Сурет 39 - «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» ШҚҚЖ баптау терезесі



Сурет 40 - Авторлар және «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» ШҚҚЖ туралы ақпарат

Есептеу эксперименттері мен практикалық сынақ мәліметтері барысында [90-95] ұсынылған модель бисызықты функциялар арқылы тәуелді қозғалыстарды адекватты сипаттауға мүмкіндік беретіні анықталды. Бұл ЖОО АББО қорғау жүйесін және киберқауіпсіздік жүйесін дамуын қаржыландыруды жоспарлайтын жоғары оқу орындарының басшылығы үшін тиімді әдіс. Қолданыстағы модельдермен салыстырғанда, ұсынылған шешім инвестор үшін тиімділік және болжау көрсеткіштерін орта есеппен 11-15% жақсартады [56-62,93-95]. Ғылыми жұмыстарды (1-тарауды қараңыз) және ақпаратты қорғау жүйелерін математикалық модельдеуге арналған қолданыстағы бағдарламалық өнімдерді талдау, сондай-ақ біздің ШҚҚЖ модульдерін тестілеу және сынақтан өткізу «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» ШҚҚЖ және «DSS ШҚҚЖ (АҚЖ таңдау үшін Парето әдісі)» - негізгі модульдердің бірнеше артықшылықтары бар екенін көрсетті (кесте 10).

Диссертациялық жұмыстың осы бөлімінде алынған нәтижелердің ғылыми және практикалық жаңалығы, бисызықты дифференциалдық ойындардың жаңа класын қолдануға негізделген бағдарламалық өнімнің алғаш рет құрылғандығында. Бұл класс процесті адекватты сипаттауға және ЖОО АББО-ны қорғаушы тарапына киберқауіпсіздік құралдарын қаржыландырудың оңтайлы стратегиясын табуға мүмкіндік берді.

Кесте 10 - Ақпараттандыру нысандарының ақпараттық қауіпсіздігін және киберқауіпсіздігін инвестициялау нәтижелерін болжау үшін математикалық модельдер мен бағдарламалық өнімдердің салыстырмалы сипаттамасы (атап айтқанда ЖОО АББО)

Салыстырылатын критерийлер / Модель / Бағдарламалық өнім, Өндіруші ел	**Қорғау ресурстары ескерілді**	**Шабуылдаушылардың ресурстары ескерілді**	**Жеке қорғаныс құралының құны ескерілген**	**Қазақ тіліндегі нұсқасы**	**Интерфейстің ыңғайлылығы**	**Құны, шартты өлшем**
Гросс моделі / "COMFAR" бағдарламасы (3.0 нұсқасы), РФ)	+	+	-	-	+	**120**
Гордон-Лоеб моделі / "Альт - Инвест" бағдарламасы, РФ	+	-	-	-	-	**150**
Задираки моделі / (Бағдарламалық өнім жоқ)	+	-	-	-	-	-
Глушак-Новиков моделі / (Бағдарламалық өнім жоқ)	+	-	+	-	-	-
Журиленко моделі / (Бағдарламалық өнім жоқ)	+	-	-	-	-	+
Архипов моделі / "Риск-Калькулятор" бағдарламасы, Украина	+	+	+	-	-	**0**
Хорошка-Хохлачов моделі Модель MathLab, MathCAD жасалған	-	-	-	-	-	-
Құрылған модельдер мен бағдарламалық өнімдер, Казахстан, Украина СППР «DSS» бағдарламасы	+	+	+	+	+	**0**

Алынған нәтижелердің практикалық маңыздылығы, VisualStudio 2017 бағдарламалау ортасында шешімдерді қабылдауды қолдау жүйесі үшін «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» модулінің құрылуында. "DSS" модулінде ұсынылған модель, атап айтқанда дифференциалды ойындар теориясының әдістерін қолдануға негізделген модель жүзеге асырылды. Құрылған модуль болжау мәліметтері мен ЖОО АББО-ның ақпаратты қорғау және КҚ құралдарын инвестициялаудан нақты қайтарымы арасындағы айырмашылығын азайтуға мүмкіндік береді. Шешім ЖОО АББО үшін киберқауіпсіздік құралдарын қорғаушы тарапына қаржыландырудың оңтайлы стратегиясын алуға мүмкіндік береді. ШҚҚЖ модулін бағдарламалық жүзеге асыру ЖОО АББО-ның қорғау

периметрлерін бұзуға әрекет ететін екінші тарап қаншалықты қаржыландыру жасаса да, қаржыландыру процесін сипаттайтын параметрлердің кез- келген қатынасында қорғаушы тарапқа оңтайлы қаржы стратегиясын таңдауға мүмкіндік береді. «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» ШҚҚЖ модулінің бағдарламалық коды келтірілген (Қосымша Ә).

Төртінші тарау бойынша қорытындылар:

– Жоғары оқу орнының ақпараттық білім беру ортасының қорғалуын бағалау есептерін шешу үшін көпкритериалды дискретті оңтайландырудың әдісі жетілдірілді. Шешім Эджворт-Парето дискретті оңтайландыру әдісімен лексикографиялық әдісті байланыстыруға негізделген. Құрамында оңтайлылықтың екі шарты бар шешімді бағалаудың векторлық критерийі жасалды: ЖОО АББО үшін ТКҚ-да немесе АҚЖ-да қарастырылып отырған нұсқаларының құндық бағасы және нақты модификациялардың техникалық тиімділігін бағалау.

– ЖОО АББО-ның ақпараттық қауіпсіздік және киберқауіпсіздік жүйесін жүзеге асырудың барлық ықтимал нұсқаларын ескере отырып, ЖОО АББО үшін ТКҚ-ны мен АҚЖ-ны жобалау кезінде оңтайлы таңдау алгоритмдері құрылды және сынақтан өткізілді.

– Жоғары оқу орнының ақпараттық білім беру ортасы үшін ТКҚ және АҚЖ жобалау кезінде оңтайлы таңдау алгоритмдерін жүзеге асыратын «ШҚҚЖ (АҚЖ таңдау үшін Парето әдісі)» модулі компьютерлік бағдарламасы құрылды.

– Бисызықты дифференциалдық ойындардың жаңа класын қолдануға негізделген бағдарламалық өнім құрылды. Бұл класс процесті адекватты сипаттауға және ЖОО АББО-ның қорғаушысына киберқауіпсіздік құралдарын қаржыландырудың оңтайлы стратегиясын табуға мүмкіндік берді. VisualStudio 2017 бағдарламалау ортасында шешімдерді қабылдауды қолдау жүйесі - «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» үшін модуль құрылды. «DSS» модулінде дифференциалды ойындар теориясының әдістерін қолдануға негізделген модель іске асырылды. Құрылған модуль болжау мәліметтері мен ЖОО АББО-ның ақпаратты қорғау және КҚ құралдарын инвестициялаудан нақты қайтарымы арасындағы айырмашылығын азайтуға мүмкіндік береді. Шешім қорғаушы тарапқа ЖОО АББО үшін киберқауіпсіздік құралдарын қаржыландырудың оңтайлы стратегиясын алуға мүмкіндік береді. ШҚҚЖ модулін бағдарламалық жүзеге асыру ЖОО АББО-ның қорғау периметрлерін бұзуға әрекет ететін екінші тарап қаншалықты қаржыландыру жасаса да, қаржыландыру процесін сипаттайтын параметрлердің кез- келген қатынасында қорғаушы тарапқа оңтайлы қаржы стратегиясын таңдауға мүмкіндік береді.

ҚОРЫТЫНДЫ

Жұмыста төмендегідей негізгі нәтижелер алынды:

– жоғары оқу орындарының ақпараттық білім беру ортасын (ЖОО АББО) қорғауды қамтамасыз ету саласындағы алдыңғы зерттеулерге шолу және талдау жүргізілді;

– әлемде көптеген өнеркәсіптері дамыған мемлекеттерде цифрлық білім беру жүйесінің дамуындағы артықшылығы тек қана педагогикалық қызмет саласындағы мамандарға ғана емес, ақпаратты қорғау және киберқауіпсіздік проблемаларын ескере отырып ақпараттық технологиялар мамандарына да сәйкес техникалық – әдістемелік қолдауды талап ететіні көрсетілді;

– көптеген мемлекеттерде ақпараттық ресурстарға қолжетімділікті жаһандандыруды дамытудың қалыптасқан түрі заманауи жоғары оқу орындарының қызметтерінің барлық салаларына жаңа цифрлық және ақпараттық - коммуникациялық технологияларды енгізу есебінің өзекті екені негізделді;

– жоғары оқу орындарының ақпараттық білім беру ортасының киберқауіпсіздік жүйесіндегі инвестициялық процесс параметрлерінің әртүрлі қатынасын ескере отырып инвестициялауды басқару стратегияларын табу бойынша шешімдерді қабылдауды қолдау жүйесі үшін модель әзірлеу бағытындағы зерттеулердің өзектілігі негізделген;

– жоғары оқу орындарының ақпараттық білім беру ортасының киберқауіпсіздік стратегияларында инвестициялауды басқару стратегияларын табу бойынша есептерді шешуге компьютерлік қолдау көрсету қажеттілігі көрсетілді;

– жоғары оқу орындарының ақпараттық білім беру ортасының ақпаратты қорғау жүйесін және киберқауіпсіздік жүйесін инвестициялаудың рационалды қаржы стратегиясын таңдау бойынша шешімдер қабылдауды қолдау интеллектуалданған жүйесі үшін жаңа модель ұсынылды. Модельде ақпараты толық берілмеген есепті шешу үшін динамикалық бағдарламалау әдісі қолданылады. Бұл қолданыстағы шешімдерге қарағанда, ЖОО АББО-ны қорғаушы тарапына ақпараттық жүйелерді қорғау кезінде ресурсттардың шығындарын талап ететін жағдайлардың нұсқалары үшін шешімдерді неғұрлым тиімді табуға мүмкіндік берді;

– есептеу эксперименттерінің нәтижелері сипатталған. Ойынның шешімі ЖОО АББО-ны қорғаушы және ЖОО АББО-ның киберқауіпсіздік шекарасын өтуге ұмтылатын компьютер қаскүнемдері жағынан ойыншылардың ойын параметрлер қатынасының барлық жағдайлары үшін келтірілген. ЖОО АББО-ны қорғаушының оңтайлы әрекеттерінің (қаржы стратегияларының) нұсқалары табылды. Есептеу эксперименттері барысында ұсынылған математикалық модельдердің сайлылығы дәлелденді. Есептеу эксперименттері нәтижелерінің практикалық мәліметтерден ауытқуы 12% - дан аспайды;

– жоғары оқу орынының ақпараттық білім беру ортасының киберқорғауын бейімделген басқарудың тұжырымдамалық моделі сипатталды;

– Петри желілерінің аппаратын пайдалана отырып, қолданушылардың қолжетімділік құқықтарын бейімдеу басқару есептерінің шешімі бірінші рет сипатталған. Оған сәйкес келетін модель жүзеге асырылды және PIPE v4.3.0 және Petri.NetSimulator. 2.017 пакеттерде имитациялық модельдеу орындалды;

– жоғары оқу орындарының ақпараттық білім беру ортасындағы киберқатерді азайту немесе бейтараптандыру үшін қолданушының профилін нақтылау процедураларын автоматтандырудың алғашқы моделі ұсынылды. Ақпараттандыру объектілерінің компьютерлік желілерінде қолданушылар тағайындаған есептерді үлестіру (мәселелерді бөлу) моделі даму алды. Модель үшін база Петри желілерінің математикалық аппараты болды. Модельдің қолданыстағы модельдерге қарағанда айырмашылығы, бұл модельде күйдің ішкі кеңістігінің қуатын азайтуға мүмкіндік беретін айнымалылар бар. Сондай-ақ, модельдеудің нәтижелілігі, атап айтқанда қолжетімділік құқықтарын реттеуге байланысты шешімдер қабылдауға кететін уақыт шығындарын қысқарту есебінен жоғарылады;

– қолжетімділік құқықтарын бақылау әдісі нақтыланды және толықтырылды. Қауіпсіздік саясатының мәселелері мен талаптары сұранысының қолжетімділік құқықтарын салыстырып тексеру аспектілеріне қатысты нақтылаулар болды. Сонымен қатар, ЖОО АББО-ның мәселелері мен қолжетімділікке рұқсат етілген төбелердің сәйкестігі ескерілді. ЖОО АББО-ның төбелері үшін де тиісті құқықтары бар абоненттер үшін қолжетімділік құқығын салыстыру процедурасы қарастырылған. Модель жоғары оқу орнының нақты ақпараттық білім беру ортасы үшін қауіпсіздік саясатының ағымдағы көрсеткіштерін және соңғыларын нақтылау мүмкіндігі бар қауіпсіздік метрикасын ескереді. Жаңа мәселелер немесе қайта қарастырылатын мәселелер үшін қауіпсіздік ережелері мен метрикаларын нақтылау Петри желілерінің шартты белгілерінде сипатталған;

– жоғары оқу орнының ақпараттық білім беру ортасының қорғалуын бағалау есептерін шешу үшін көпкритериалды дискретті оңтайландырудың әдісі жетілдірілді. Шешім Эджворт-Парето дискретті оңтайландыру әдісімен лексикографиялық әдісті байланыстыруға негізделген. Құрамында оңтайлылықтың екі шарты бар шешімді бағалаудың векторлық критерийі жасалды: ТКҚ- да немесе АҚЖ-да қарастырылып отырған нұсқаларының құндық бағасы және нақты ЖОО АББО үшін модификациялардың техникалық тиімділігін бағалау. ЖОО АББО-ның ақпараттық қауіпсіздік және киберқауіпсіздік жүйесін іске асырудың барлық ықтимал нұсқаларын ескере отырып, ЖОО АББО үшін ТКҚ-ны мен АҚЖ-ны жобалау кезінде оңтайлы таңдау алгоритмдері әзірленді және сынақтан өткізілді;

– жоғары оқу орнының ақпараттық білім беру ортасы үшін ТКҚ-ны және АҚЖ-ны жобалау кезінде оңтайлы таңдау алгоритмдерін жүзеге асыратын

«ШҚҚЖ (АҚЖ таңдау үшін Парето әдісі)» модулі компьютерлік бағдарламасы әзірленді;

– бисызықты дифференциалдық ойындардың жаңа класын қолдануға негізделген бағдарламалық өнім әзірленді Бұл класс процесті адекватты сипаттауға және ЖОО АББО-ның қорғаушысына киберқауіпсіздік құралдарын қаржыландырудың оңтайлы стратегиясын табуға мүмкіндік берді. VisualStudio 2017 бағдарламалау ортасында шешімдерді қабылдауды қолдау жүйесі үшін, «ЖОО АББО-ның киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау (DSS)» үшін модуль әзірлегенді. "DSS" модулінде дифференциалды ойындар теориясының әдістерін қолдануға негізделген модель іске асырылды. Әзірленген модуль болжау мәліметтері мен ЖОО АББО-ның ақпаратты қорғау және КҚ құралдарын инвестициялаудан нақты қайтарымы арасындағы айырмашылығын азайтуға мүмкіндік береді. Шешім қорғаушы тарапқа ЖОО АББО үшін киберқауіпсіздік құралдарын қаржыландырудың оңтайлы стратегиясын алуға мүмкіндік береді ШҚҚЖ модулін бағдарламалық жүзеге асыру ЖОО АББО-ның қорғау периметрлерін бұзуға әрекет ететін екінші тарап қаншалықты қаржыландыру жасаса да, қаржыландыру процесін сипаттайтын параметрлердің кез- келген қатынасында қорғаушы тарапқа оңтайлы қаржы стратегиясын таңдауға мүмкіндік береді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Балықбаев Т.О., Бидайбеков Е.Ы., Ахметов Б.С., Гришкун В.В Абай атындағы Қазақ ұлттық педагогикалық университетін цифрландыру тұжырымдам асы /Алматы: Абай атындағы ҚазҰПУ: «Ұлағат» баспасы.- 2020.- Б-109.

2 Зегжда П.Д., Полтавцева М.А., Лаврова Д.С. Систематизация киберфизических систем и оценка их безопасности // Проблемы информационной безопасности. Компьютерные системы. – СПб. -2017. -№ 2. -С. 127-138.

3 Kazmirchuk S., Lakhno V., Kovalenko Y., Myrutenko L., Zhmurko T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features // Eastern European journal of advanced technologies. –Kharkov. - 2016. - № 3(9). - С. 30-38.

4 Korchenko A., Akhmetov B., Kazmirchuk S., Chasnovskiy Ye. Система оценивания рисков информационной безопасности //Ukrainian Scientific Journal of Information Security. Киев. - 2017. -Vol. 23. Iss. 2. -P. 145-152.

5 Котенко И.В., Юсупов Р.М. Перспективные направления исследований в области компьютерной безопасности // Защита информации. – Киев. -2006.-№2.-С. 46-57.

6 Atighetchi M., Adaptive Cyberdefenese for Survival and Intrusion Tolerance //Proccedins of 3 rd International Workshop Distributed Auto- adaptive and Reconfigurable Systems. – USA.-2003.- P. 74-84.

7 Campbell R.H., Yan M., Sprabery R., Gopireddy B., Fletcher C.W. Attack directories, not caches: Side channel attacks in a non-inclusive world //IEEE Symposium on Security and Privacy. - 2019. -P. 888-904.

8 Dawkins J., Clark K., Manes G. A Framework for Unified Network Security Management: Identifying and Tracking Security Threats on Converged Networks //Journal of Network and Systems Management. -2005.- Vol. 13.- No. 3.-P. 253–267.

9 Марков А.С., Барабанов А.В., Цирлов В.Л. О систематике информационной безопасности цепей поставки программного обеспечения //Безопасность информационных технологий.- М.- 2019. -Т. 26.- № 3. -С. 68-79.

10 Endler M., Talavera L., Vasconcelos I., Vasconcelos R., Cunha M. The mobile hub concept: Enabling applications for the internet of mobile things// IEEE International Conference on Pervasive Computing and Communication Workshops.- 2015.-P.123-128.

11 Lakhno V., Kartbaev T., Doszhanova A., Malikova F., Alimseitova Zh. Algorithm and Improved Methodology for Clustering Data with Self-learning Elements for Intrusion Detection Systems//Proceedings of the Computational Methods in Systems and Software, Springer, Cham. – 2019. - P. 165-173.

12 Ахметов Б.С., Тукеев У.А. Технология ситуационного управления информационной безопасностью учебного процесса казну имени Аль-Фараби

/ Журнал математики, механики и информатики. – Алматы. -2009.-Vol. 63.-N. 4.- P.- 66-70.

13 Kalimoldayev M.N., Biyashev R.G., Rog O.A. Применение логики для построения моделей разграничения доступа к информации// Доклады Национальной академии наук Республики Казахстан. – Almaty. - 2017.-, Vol.3 – Num. 313 (2017).-P. 48 – 54.

14 Утепбергенов И.Т., Яворский В.В., Байдикова Н.В., Чванова А.О. Разработка метода представления транспортной системы на основе теории гиперсетей для проектирования и управления//Материалы XIV Международной Азиатской школы-семинара «Проблемы оптимизации сложных систем.- Алматы. - 2018. -Ч. 2. -С. 333-341.

15 Хуторской А.В. Человек и его изменение в телекоммуникационных системах / Материалы Всерос. науч.-практ. конф.- М. – 2004. - С. 145 – 152.

16 Кечиев Л. Н., Путилов Г. П., Тумковский С. Р. Методы и средства построения образовательного портала технического вуза // Открытое образование. – М. - 2002.- № 2. – С. 34–42.

17 Абрамян Г.В. Теоретические основы профессионального становления педагога в информационной среде: дис. … док. пед.наук: 13.00.08 – М.- 2001.- 511 с.

18 Захарова И.Г. Формирование информационной образовательной среды высшего учебного заведения: дис. … док.пед.наук: 13.00.01– М.- 2003.-399 с.

19 Бидайбеков Е.Ы. О подготовке специалистов по информатике и информатизации образования в Республике Казахстан //Технология высшего образования в XXI веке: проблемы и перспективы развития: сб. материалов международной научно-практической конференции.- Актобе. - 2002. - С. 62-65.

20 Ахметов Б. С., Бидайбеков Е.Ы., Казмагамбетов А.Г. Влияние методической системы обучения на разработку и применение средств информатизации в вузе //Международный конгресс конференций «информационные технологии в образовании». – М. - 2003.- С. 112-113.

21 Вараменко Я.А., Яламов Г.Ю. Формирование информационно-образовательной среды колледжа с использования современных информационных систем // Сетевое издание «Управление образованием: теория и практика».- 2017. - № 4.- С. 25-39.

22 Akhmetov B., Lakhno V., Boiko Y., Mishchenko A. Designing a decision support system for the weakly formalized problems in the provision of cybersecu-rity //Eastern-European Journal of Enterprise Technologies. – 2017.-N. 1(2(85)).- P. 4-15.

23 Есиков О.В., Есиков Д.О. Математические модели и алгоритмы обеспечения сохранности информации в системах хранения и обработки данных //Известия ТулГУ. Технические науки. -2013. Вып.- 9.- Ч.2.- С. 110-118.

24 Малюк А.А. Теория защиты информации: учебное пособие для вузов/ М.: Горячая линия-Телеком. -2004. — 280 С.

25 Петров А.А. Модель выбора оптимального состава системы защиты информации в компьютерных сетях // Вестник Восточно украинского национального университет уимени Владимира Даля. – Киев.- 2013. -15 (1). - С. 166-171.

26 Ortalo R., Deswarte Y., Kaaniche M. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security // IEEE Transactions on Software Engineering. – 1999. – Vol. 25. – P. 633 – 650.

27 Puhakainen P., Siponen M. Improving employees' compliance through information systems security training: an action research study // MIS Quarterly. - 2010. -Vol. 34. - Issue 4. -P. -767.

28 Хорошко В., Грищук Р., Піскун С., Хохлачова Ю. Ігрові методи аналізу кібератак на інформаційну сферу // Захист інформації.-Киев. - 2012.-№1, -С. 1-16.

29 Акиншин Р.Н., Ивутин А.Н., Есиков Д.О., Страхов И.А. Применение математического аппарата сетей Петри-Маркова для определения временных и вероятностных характеристик системы управления высоконагруженными веб-порталами с повышенной отказоустойчивостью //Научный Вестник. - М. -2014.- № 210.-С. 85-90.

30 Gordon L., Loeb L. ZhouInvesting in cybersecurity: insights from the Gordon-Loeb model// J. Inf. Secur. -2016. - 7(02). -P. 49- 55.

31 Gordon L., Loeb M., Zhou L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model// Journal of Information Security. – 2004. - 7(02). - P. 13-19.

32 Ахметов Б.С., Тимошенко О.І., Кыдыралина Л.М. Состояние, перспективы и основные направления развития кибербезопасности информационной образовательной среды университетов // Тезисы докладов участников IV междунар. научно-практической. конф. «Актуальные вопросы обеспечения кибербезопасности и защиты информации» - Киев. 2018. – С.15- 16.

33 Кыдыралина Л.М. Жоғары оқу орнының ақпараттық - білім беру ортасының киберқауіпсіздігін өзара қаржыландыру бойынша шешімдерді қолдау //Абай атындағы ҚазҰПУ Хабаршысы, «Физ.-мат.» сериясы. – Алматы. 2018. - №4(64), - Б. 54-58.

34 Kydyralina L.M., Akhmetov B.B., Lakhno V.A.,Adranova A.B. Review and analysis of previous researches in the sphere of ensuring the protection of information and educational environment of universities //Bulletin of National academy of sciences of the Republic of Kazakhstan.- Almaty. - 2019. – Vol. 4. – Num. 380 (2019). – P. 154 – 169.

35 Кыдыралина Л.М. Предпосылки для формирования безопасной информационно-образовательной среды современного университета // «Защита информации». – Киев. 2018. -ТОМ 20, №4, - С. 205-214.

36 Ахметов Б.С., Лахно В.А., Глазунова О.Г., Кыдыралина Л.М. The main directions of development of cyber-security of the information educational environment

of universities // Материалы Международной научно-практической. конф. «Цели устойчивого развития третьего тысячелетия».– Киев. 2018. - С. 411-413.

37 Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Decision support approaches for cyber security investment // Decision Support Systems.-2016.- Vol. 86.- P. 13–23.

38 Gamal M. M., Hasan B., Hegazy A. F. A Security Analysis Framework Powered by an Expert System// International Journal of Computer Science and Security. – 2011. - Vol. 4. - N. 6. -P. 505–527.

39 Chang LiYun, Lee Zne-Jung. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system//International Conference on Fuzzy Theory and Its Applications.- 2013.- P. 346 – 351.

40 Lakhno, V., Petrov, A., & Petrov, A. Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport//In International Conference on Information Systems Architecture and Technology- 2017.- P. 113-127.

41 Carlton M. & Levy Y. Expert assessment of the top platform independent cybersecurity skills for non-IT professional// InSoutheastCon – 2015.- P. 1–6.

42 Johnson A.M. Business and security executives views of information security investment drivers: Results from a Delphi study//Journal of Information Privacy and Security- 2009.- 5(1). -P. 3–27.

43 Chaturvedi M., Singh A. N., Gupta M. P., Bhattacharya J. Analyses of issues of information security in Indian context//Transforming Government: People, Process and Policy- 2014.- Vol. 8.- Iss.3.-P.374–397.

44 Lakhno V., Boiko Y., Mishchenko A., Kozlovskii V. , Pupchenko O. Development of the intelligent decision-making support system to manage cyber protection at the object of informatization//Eastern-European Journal of Enterprise Technologies. -2017. - №.2 (9(86)). - P. 53–61.

45 Akhmetov B., etc. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity//Eastern-European Journal of Enterprise Technologies -2017. - №1 (2 (85)).- P. 4–15.

46 Akhmeto B., etc. The choice of protection strategies during the bilinear quality game on cyber security financing// Bulletin of the national academy of sciences of the republic of Kazakhstan -2018.-№.3.- P. 6–14.

47 Akhmetov B., etc. Model of cyber security financing within the framework of the bilinear differential quality game scheme// Radio Electronics, Computer Science, Control -2018.-№.3.- P. 17–26.

48 Akhmetov, B. S., Korchenko, A. G., Kazmirchuk, S. V., & Zhekambayeva, M. N. Methods of estimation of risks for control systems of information security// Bulletin of the national academy of sciences of the republic of Kazakhstan. - 2015. - №.6. -P. 23–38.

49 Shaikhanova A., Shangytbayeva G., Ahmetov B., Beisembekova R. //Comparison of Methods of Treatment of Fuzzy Information for Distribution of Access in Computer Systems// Research Journal of Applied Sciences, Engineering and Technology. - 2015. - N.10(9). -P. 1082–1088.

50 Lakhno V. A., Petrov O. S., Hrabariev A. V., Ivanchenko Y. V.,Beketova G. S. Improving of information transport security under the conditions of destructive influence on the information-communication system//Journal of theoretical and applied information technology. - 2016.-N. 89(2).- P. 352–362.

51 Lakhno V. A., Kravchuk P. U., Pleskach V. L., Stepanenko O. P., Tishchenko R. V., Chernyshov V. A. Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems//Journal of Theoretical and Applied Information Technology. - 2017.-N. 95(8), -P. 1705–1714.

52 Akhmetov B. etc., Decision support system about investments in smart city in conditions of incomplete information// International Journal of Civil Engineering and Technology. - 2019. -N. 10 (2). -P. 661–670.

53 Bidiuk P.I., Prosiankina-Zharova T.I., Terentieev O.M., etc. Intellectual technologies and decision support systems for the control of the economic and financial processes// Journal of Theoretical and Applied Information Technology. – 2019. -№. 97 (1). - P. 71– 87.

54 Akhmetov B., etc. Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity// Advances in Intelligent Systems and Computing. -2019.- №.86. P. 162–171.

55 Akhmetov B. etc. Models and algorithms of vector optimization in selecting security measures for higher education institution’s information learning environment// Advancesin Intelligent Systems and Computing. - 2019. -№. 860, - P. 135–142.

56 Ахметов Б.С., Лахно В.А., Кыдыралина Л.М. Выбор стратегий финансирования систем кибербезопасности информационно образовательной среды университета // Тезисы докладов участ. X Всеукраинськои наук. - практической. конф. «Состояние и удоскон. безопасности инфор - телекоммун. систем». – Коблево. - 2018. - С. 8-9.

57 Кыдыралина Л.М., Ахметов Б.С., Лахно В.А. Моделирование процедуры принятия решений по финансированию средств кибербезопасности информационно-образовательной среды университета //«Защита информации ». – Киев. - 2018. –Т. 20, №2, - С. 120-127.

58 Akhmetov B., Kydyralina L., Lakhno V., Mohylnyi G., Akhmetova J, Tashimova A. Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions // International Journal of Mechanical Engineering and Technology. – 2018. – Vol.9.– Iss.10.– P. 1114–1122.

59 Ахметов Б.С., Кыдыралина Л.М. Модель интеллектуальной системы поддержки решения по финансовым вложениям в кибербезопасность

информационно-образовательной среды университета // Сборник статей XV Междунар. науч.-тех. конф. «Новые информационные технологии и системы». – Пенза. - 2018. - С. 64-67.

60 Akhmetov B., Lakhno V., Kydyralina L., Malyukov V., Kartbaeyv T., Tussupova B., Doszhanova A. Optimization of decision-making on financing of means of cyber security in the conditions of the fissile counteraction to the attacking party // International Journal of Civil Engineering and Technology. - 2019. – Vol. 10. – Iss. 03. - P. 1435-1446.

61 Кыдыралина Л.М. Оқу орнының киберқауіпсіздік құралдарын қаржыландыру бойынша шешімдерді қолдау моделі/ Абай атындағы ҚазҰПУ Хабаршысы, «Физ.-мат.» сериясы. – Алматы.- 2018. - №3(63). - Б. 401-406.

62 Lakhno V., Malyukov Y., Yerekesheva M., Kydyralina L.,Sarsimbayeva S., Zhumadilova M., Buriachok V., Sabyrbayeva G. Model of cybersecurity means financing with the procedure of additional data obtaining by the protection side // Journal of Theoretical and Applied Information Technology. – 2020. - Vol. 98. - Iss. 1. - P. 1-14.

63 Brij G., Dharma Agrawal P., Yamaguchi S. eds. Handbook of research on modern cryptographic solutions for computer and cyber security// IGI Global. - 2016.- P. 34-40.

64 Jasiul B., Szpyrka M., Śliwa, J. Detection and modeling of cyber attacks with Petri nets// Entropy. -2014. -N.16(12). -P.6602–6623.

65 Liu X., Zhang J., Zhu P. Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory// International Journal of Critical Infrastructure Protection. - 2017. - N.16. - P.13–25.

66 Jasiul B., Szpyrka M., Śliwa, J. Formal specification of malware models in the form of colored Petri nets// In Computer Science and its Applications. - 2015. - P. 475–482.

67 Akhmetov B., Lakhno V., Boiko Y., Mishchenko A. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity//Eastern-European Journal of Eenterprise Technologies. - 2017. - N.1(2). – P. 4–15.

68 Arendt D. L., Burtner R., Best D. M., Bos N. D., Gersh J. R., Piatko C. D., Paul, C. L. Ocelot: user-centered design of a decision support visualization for network quarantine // In Visualization for Cyber Security. – 2015.- P. 1–8.

69 Alheeti K. M., Gruebler A., McDonald-Maier K. D., Fernando A. Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model// In Consumer Electronics. – 2016. - P. 502–503.

70 Carvalho M. A., Bandiera-Paiva P. Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri Nets modeling// In Security Technology. – 2017. - P. 1–8.

71 Narayanan M., Cherukuri A. Verification of Cloud Based Information Integration Architecture using Colored Petri Nets// International Journal of Computer Network and Information Security. – 2018. – N.10(2). – P. 10-16.

72 Lakhno V. A., Tkach Y. N., Petrenko T.A., Zaitsev S.V., Bazylevych V. M. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks// Eastern-European Journal of Enterprise Technologies. – 2016. – N. 6/9 (84). - P. 32–44.

73 Beketova G., Akhmetov B., Korchenko A., Lakhno V, Tereshuk A. Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition// Computer modelling and new technologies. – 2017. – Vol. 21.- N. 2. - P. 7–16.

74 Ахметов Б.С., Кыдыралина Л.М. Модель на основе сети Петри для разграничения полномочий пользователей в сети информационно-образовательной среды университета //Сборник статей XVIII Международная науч.-тех. конф. «Проблемы информатики в образовании, управлении, экономике и технике». – Пенза. - 2018. - С. 81-83.

75 Lakhno V., Buriachok V., Parkhuts L., Tarasova H., Kydyralina L., Skladannyi P., Skrypnyk M., Shostakovska A. Development of a conceptual model of adaptive access rights management with using the apparatus of petri nets// International Journal of Civil Engineering and Technology. - 2018. - Vol.9. - Iss. 11. - P. 95–104.

76 Ахметов Б.С., Кыдыралина Л.М. Модель на основе сети Петри для разграничения полномочий пользователей в сети информационно-образовательной среды университета //Сборник статей. XVIII Международная науч.-тех. конф. «Проблемы информатики в образовании, управлении, экономике и технике». – Пенза. -2018. - С. 81-83.

77 Akhmetov B.B., Lakhno V.A., Adranova A.B, Kydyralina L., Pliska L.D. Analysis of mathematical models of investment strategies in the university on cyber security systems//Bulletin of National academy of sciences of the Republic of Kazakhstan.- Almaty. - 2020. – Vol. 1. – N. 383 (2020). – P. 128 – 139.

78 Ахметов Б.С., Лахно В.А., Кыдыралина Л.М. Метод и модель распознавания киберугроз в электронной информационно-образовательной среде вуза /Сборник материалов Международной науч.- практ. конф. «Актуальные вопросы экономического и социального развития в условиях цифровизации». - Семей.- 2019. - С. 323-329.

79 Ахметов Б.С., Лахно В.А., Кыдыралина Л.М. Концептуальная модель адаптивного управления правами доступа в информационно-образовательной среде университета с использованием аппарата сетей Петри //« Университет-регион мнений» в рамках Yessenov Forum материалы междунар. науч.-практ. конф.– Ақтау.- 2019.- I Том, - С.315-322.

80 Ахметов Б.С., Лахно В.А., Кыдыралина Л.М. Жоғары оқу орынының электрондық ақпараттық білім беру ортасына қолданушыларды

аутентификациялау кезінде мүмкін қатерлерді талдау әдісі мен моделі/ «Математикалық модельдеу мен ақпараттық технологиялар білімде және ғылымда» атты IX Халықаралық ғылыми-әдістемелік конф. материалдары. – Алматы.- 2020. - Б. 198-204.

81 Wong K., Dillabaugh C., Seddigh N., Nandy B. Enhancing Suricata intrusion detection system for cyber security in SCADA networks// In Electrical and Computer Engineering. – 2017. – P.1–5.

82 Ivanova Y. A. Simulation modelling and assessing the impact of cyberattacks on urban automobile transport systems// International Journal on Information Technologies & Security. – 2017. – N. 9(3). – P. 117–141.

83 Moreira N., Molina E., Lázaro J., Jacob E., Astarloa A. Cyber-security in substation automation systems // Renewable and Sustainable Energy Reviews. – 2016. – N. 54. – P. 1552–1562.

84 Shvetsov A. V., Sharov V. A., Shvetsova S. V. Method of protection of pedestrian zones against the terrorist attacks made by means of cars including off-road vehicles and trucks// European Journal for Security Research. – 2017. –N.4. – P. 1-11.

85 Ahmad A., Maynard S. B., Park S. Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing. – 2014. № 25(2). -P.357–370.

86 Akhmetov B., Lakhno V., Boiko Y., Mishchenko A. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity// Eastern-European Journal of Enterprise Technologies. – 2017. –№. 1(2 (85)). – P. 4–15.

87 Lakhno V., Boiko Y., Mishchenko A., Kozlovskii V., Pupchenko O. Development of the intelligent decision-making support system to manage cyber protection at the object of informatization // Eastern-European Journal of Enterprise Technologies. – 2017. –№. 2/9 (86). - P. 53–61.

88 Lotov A., Bushenkov V., Kamenev G. Interactive decision maps: Approximation and visualization of Pareto frontier / Springer Science & Business Media, Optimality of Radio Power Control Via Fast-Lipschitz Optimization. – 2013. - Vol. 89. – Iss. 64. - P. 2589–2601.

89 Knowles W., Prince D., Hutchison D., Disso J., Jones K. A survey of cyber security management in industrial control systems//International journal of critical infrastructure protection. – 2015. – Vol. 9. – P. 52–80.

90 Podinovski V., Kuosmanen T. Modelling weak disposability in data envelopment analysis under relaxed convexity assumptions//European Journal of Operational Research. – 2011. – N. 211.3. - P. 577–585.

91 Collette Y., Siarry P. Multiobjective optimization: principles and case studies// Springer Science & Business Media, Novel Solution Approach for Multi-Objective Attack-Defense Cyber Games With Unknown Utilities of the Opponent. – 2017. – N. 1(1). – P. 16–26.

92 Lakhno, V. A., Kravchuk, P. U., Pleskach, V. L., Stepanenko, O. P., Tishchenko, R. V., &Chernyshov, V. A. Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems// Journalof Theoretical and Applied Information Technology. – 2017. – N. 95(8). –P. 1705-1714.

93 Ахметов Б.С., Лахно В.А., Адранова А.Б., Кыдыралина Л.М. Жоғары оқу орнының ақпараттық білім беру ортасын қорғау құралдарын таңдаудың векторлық оңтайландыру модельдері мен алгоритмдері/ Абай атындағы ҚазҰПУ Хабаршысы, «Физ.-мат.» сериясы. – Алматы. - 2018. - №1(61), - Б. 244-250.

94 Akhmetov B., Lakhno V., Akhmetov B., Myakuhin Y., Kydyralina L. Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution's Information Learning Environment //Intelligent Systems in Cybernetics and Automation Control Theory. Warsaw. - 2018. - Vol. 860. P.135-142.

95 Ахметов Б.С., Лахно В.А., Кыдыралина Л.М. Алгоритм выбора технических средств охраны и кибербезопасности объектов информатизации/Тезисы конференции XIX Международная науч.-техн. конф. «Проблемы техники и технологий телекоммуникаций». – Уральск. - 2018. - С. 219-221.

ҚОСЫМША А

«ШҚҚЖ модулі (АҚЖ таңдау үшін Парето әдісі)» бағдарламалық өнімнің коды

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Text.RegularExpressions;

namespace pareto_form
{
   public partial class Form1 : Form
   {
      static List<double> Q = new List<double>();
      static List<double> V = new List<double>();
      static List<int> Selected = new List<int>();
      static List<int>SelectedMax = new List<int>();
      static List<int>SelectedV = new List<int>();
      static List<int>SelectedQ = new List<int>();
      static int S = 0;
      static double q_por = 0, V_por = 0, a1 = 0, a2 = 0;
      static Random rand = new Random();

      public void random_calculation()
      {
         for (inti = 0; i< S; i++)
         {
Q.Add(rand.Next(0, 999) * 0.001);
V.Add(rand.Next(100, 999));
         }
      }

      public List<double>readQuality()
      {
interr_count = 0;
         if (string.IsNullOrWhiteSpace(readQualityTextBox.Text) == false)
         {
            try
            {
               Q = Regex.Matches(readQualityTextBox.Text, @"([^\s]+)\s*").OfType<Match>()
.Select(mt =>double.Parse(mt.Groups[0].Value))
.ToList();
            }
catch
            {
MessageBox.Show("Введено неверное значение эффективности для СЗИ!",
```

```
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
        }
        for (inti = 0; i<Q.Count(); i++)
        {
           if (Q[i] <= 0 || Q[i] >= 1)
           {
err_count++;
}
        }
if (err_count != 0)
        {
MessageBox.Show("Введено неверное значение эффективности для СЗИ!",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
        if (Q.Count() != 0)
        {
readValueTextBox.ReadOnly = false;
        }
        return Q;
      }


      public List<double>readValue()
      {
interr_count = 0;
        if (string.IsNullOrWhiteSpace(readValueTextBox.Text) == false)
        {
           try
           {
              V = Regex.Matches(readValueTextBox.Text, @"([^\s]+)\s*").OfType<Match>()
.Select(mt =>double.Parse(mt.Groups[0].Value))
.ToList();
           }
catch
           {
MessageBox.Show("Введено неверное значение эффективности для СЗИ!\nДолжно выполняться условие
0<Q<1",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
        }
        for (inti = 0; i<V.Count(); i++)
        {
           if (V[i] <= 100 || V[i] >= 1000)
           {
err_count++;
}
        }
if (err_count != 0)
        {
MessageBox.Show("Введено неверное значение стоимости для СЗИ!\nДолжно выполняться условие
100<V<1000",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
```

```
}
        if (Q.Count() != V.Count())
{
MessageBox.Show("Количество объектов для эффективности и стоимости должно быть одинаковым!",
              "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
        return V;
      }
      public Form1()
      {
InitializeComponent();
objectsGridView.Font = new Font("Century Gothic", 9);
      }
      private void importantCriterionYESradioButton_Click(object sender, EventArgs e)
      {
         a1_weight_textBox.Visible = true;
         a2_weight_textBox.Visible = true;
Q_weight_label.Visible = true;
V_weight_label.Visible = true;
      }
      public void clearAll()
      {
objectsGridView.Rows.Clear();
         result1TextBox.Clear();
         result2TextBox.Clear();
         result3TextBox.Clear();
         result4TextBox.Clear();
         maxResult1TextBox.Clear();
         maxResult2TextBox.Clear();
         maxResult3TextBox.Clear();
         maxResult4TextBox.Clear();
      }

      private void execute_Click(object sender, EventArgs e)
      {

clearAll();

         if (inputMethodRadioButton1.Checked)
         {
random_calculation();
         }
         else
         {
readQuality();
readValue();
         }

         if (V_por_textBox is null || Q_por_textBox is null || CountTextBox is null || Q.Count() == 0 || V.Count()
== 0)
{
MessageBox.Show("Заданы не все исходные данные!",
   "Некорректные исходные данные!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
```

```
}

SearchOptimalAtFirst();
        if (Selected.Count() == 0)
        {
           result1TextBox.Text = "Оптимальныхзначенийненайдено";
        }
        else
        {
           result1TextBox.Text = String.Join(" ", Selected);
           maxResult1TextBox.Text = String.Join(" ", SelectedMax);
        }
SearchOptimalAtSecond();
        if (Selected.Count() == 0)
        {
           result2TextBox.Text = "Оптимальныхзначенийненайдено";
        }
        else
        {
           result2TextBox.Text = String.Join(" ", Selected);
           maxResult2TextBox.Text = String.Join(" ", SelectedMax);
        }

SearchOptimalAtThird();
        if (Selected.Count() == 0)
        {
           result3TextBox.Text = "Оптимальныхзначенийненайдено";
        }
        else
        {
           result3TextBox.Text = String.Join(" ", Selected);
           maxResult3TextBox.Text = String.Join(" ", SelectedMax);
        }

SearchOptimalAtFourth();
        if (Selected.Count() == 0)
        {
           result4TextBox.Text = "Оптимальныхзначенийненайдено";
        }
        else
        {
           result4TextBox.Text = String.Join(" ", Selected);
           maxResult4TextBox.Text = String.Join(" ", SelectedMax);
        }

        try
        {
           for (inti = 0; i<Q.Count(); i++)
           {
objectsGridView.Rows.Add(i, Q[i], V[i]);
}
        }
catch
```

```
        {
MessageBox.Show("Значения следует вводить через пробел.\nДля вещественных значений следует
использовать запятую. Например, 0,1.\nЗначення, щовводятьсяповинні бути більші нуля",
                "Некорректные исходные данные!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
Q.Clear();
V.Clear();
Selected.Clear();
      }
      private void infoButton_Click(object sender, EventArgs e)
{
MessageBox.Show("Программа предназначена для оптимизации выбора средств зищиты " +
            " информации, кибербезопасности и технических средств охраны " +
            " для информационно-образовательной среды университета.\n\nВ основу модели, используемой
в программе, положен усовершенствованный алгоритм векторної оптимизации " +
            "в задачах информационной и кибербезопасности.\n\nАвторы: Лахно В.А. (Украина),
Кыдыралина Л. (Казахстан)\n\n2019 г.",
"Инфо", MessageBoxButtons.OK, MessageBoxIcon.Information);
      }
      private void clear_Click(object sender, EventArgs e)
      {
clearAll();
      }
      private void readQualityTextBox_Leave(object sender, EventArgs e)
      {
readQuality();
      }

      private void readValueTextBox_Leave(object sender, EventArgs e)
      {
readValue();
      }
      private void Q_por_textBox_Leave(object sender, EventArgs e)
      {
         try
         {
q_por = Convert.ToDouble(Q_por_textBox.Text);
}
catch
         {
MessageBox.Show("Введено неверное значение граничной эффективности!",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
         if (q_por>= 1 || q_por<= 0)
{
MessageBox.Show("Введено неверное значение граничной эффективности!\nДолжно выполняться
условие 0<q_por<1",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
      }
      private void V_por_textBox_Leave(object sender, EventArgs e)
      {
         try
```

```
        {
V_por = Convert.ToDouble(V_por_textBox.Text);
}
catch
        {
MessageBox.Show("Введено неверное значение граничной эффективности!",
              "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
        if (V_por>= 1000 || V_por<= 100)
{
MessageBox.Show("Введено неверное значение граничной эффективности!\n\nДолжно выполняться
условие 100<V_por<1000",
              "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
      }

      private void CountTextBox_Leave(object sender, EventArgs e)
      {
         if (!inputMethodRadioButton2.Checked)
         {
            try
            {
               S = Convert.ToInt32(CountTextBox.Text);
}
catch
            {
MessageBox.Show("Не верно задано количество рассматриваемых элементов СЗИ",
                  "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
         }
         else
         {
            S = Q.Count();
         }
         if (S <= 0)
{
MessageBox.Show("Введена неверное количество объектов для анализа",
   "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
         }
elseif (S > 32000)
         {
MessageBox.Show("Введена слишком большое количество объектов для анализа (Максимум 32000)",
              "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
      }
      private void importantCriterionGroupBox1_Leave(object sender, EventArgs e)
      {
         if (importantCriterionYESradioButton.Checked)
         {
            try
            {
               a1 = Convert.ToDouble(a1_weight_textBox.Text);
}
```

```
catch
            {
MessageBox.Show("Введено неверное значение для коэффициента важности 0<(a1)<100!",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}
            try
            {
                a2 = Convert.ToDouble(a2_weight_textBox.Text);
}
catch
            {
MessageBox.Show("Введено неверное значение для коэффициента важности 0<(a2)<100!!",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
            }
if (a1 <= 0 || a2 <= 0 || a1 >= 100 || a2 >= 100)
            {
MessageBox.Show("Введены не верные значения!\nДолжно выполняться условие 0<(a1,a2)<100",
                "Введено неверное значение!", MessageBoxButtons.OK, MessageBoxIcon.Warning);
}

            for (inti = 0; i<Q.Count; i++)
            {
                Q[i] = Q[i] * a1;
            }

            for (int j = 0; j <V.Count; j++)
            {
                V[j] = V[j] * a2;
            }

q_por = q_por * a1;
V_por = V_por * a2;
          }
      }

      private void area1ResultLabelTextBox_Click(object sender, EventArgs e)
{
MessageBox.Show("В области I эффективность выше пороговой, а стоимость меньше
пороговой\n\nQ>Q_por i V<V_por",
"Область I", MessageBoxButtons.OK, MessageBoxIcon.Information);
      }

      private void area2ResultLabelTextBox_Click(object sender, EventArgs e)
{
MessageBox.Show("В области II эффективность и стоимость больше пороговой\n\nQ>Q_por i V>V_por",
"Область II", MessageBoxButtons.OK, MessageBoxIcon.Information);
      }

      private void area3ResultLabelTextBox_Click(object sender, EventArgs e)
{
MessageBox.Show("В области III эффективность и стоимость меньше пороговой\n\nQ<Q_por i V<V_por",
"Область III", MessageBoxButtons.OK, MessageBoxIcon.Information);
      }
```

```
        private void area4ResultLabelTextBox_Click(object sender, EventArgs e)
{
MessageBox.Show("В областi IV эффективность меньше пороговой, а стоимость больше
пороговой\n\nQ<Q_por i V>V_por",
"Область IV", MessageBoxButtons.OK, MessageBoxIcon.Information);
        }
        private void inputMethodRadioButton2_CheckedChanged(object sender, EventArgs e)
        {
readQVGroupBox.Visible = true;
Count_label.Visible = false;
CountTextBox.Visible = false;
        }
        private void inputMethodRadioButton1_CheckedChanged(object sender, EventArgs e)
        {
readQVGroupBox.Visible = false;
Count_label.Visible = true;
CountTextBox.Visible = true;
        }
        private void importantCriterionNOradioButton_Click(object sender, EventArgs e)
        {
            a1_weight_textBox.Visible = false;
            a2_weight_textBox.Visible = false;
Q_weight_label.Visible = false;
V_weight_label.Visible = false;
        }
        public static List<int>SearchOptimalAtFirst()
        {
inti, qi_max = -1;
SelectedMax.Clear();
Selected.Clear();
            double q_max = 0;
            for (i = 0; i<Q.Count(); i++)
            {
                if (Q[i] >= q_por&& V[i] <= V_por)
                {
Selected.Add(i);
                }
            }
            for (i = 0; i<Q.Count(); i++)
            {
                if (Q[i] >= q_por&& Q[i] >q_max&& V[i] <= V_por)
                {
q_max = Q[i];
qi_max = i;
                }
            }
            if (qi_max != -1)
            {
SelectedMax.Add(qi_max);
            }
            return Selected;
        }
```

```
        public static List<int>SearchOptimalAtSecond()
        {
inti, ii, vi_min = 0;
            double v_min = 99999;
SelectedMax.Clear();
Selected.Clear();
            for (i = 0; i<Q.Count(); i++)
            {
                if (Q[i] >= q_por&& V[i] >= V_por)
                {
Selected.Add(i);
                }
            }
            for (i = 0; i<Q.Count(); i++)
            {
                if (Q[i] >= q_por&& V[i] >= V_por&& V[i] <v_min)
                {
v_min = V[i];
vi_min = i;
                }
            }
            if (v_min != 99999)
            {
SelectedMax.Add(vi_min);
            }
            return Selected;
        }
        public static List<int>SearchOptimalAtThird()
        {
inti, qi_max = -1;
            double q_max = 0;
SelectedMax.Clear();
Selected.Clear();
            for (i = 0; i<V.Count(); i++)
            {
                if (V[i] <= V_por&& Q[i] <= q_por)
                {
Selected.Add(i);
                }
            }
            for (i = 0; i<V.Count(); i++)
            {
                if (V[i] <= V_por&& Q[i] <= q_por&& Q[i] >q_max)
                {
q_max = Q[i];
qi_max = i;
                }
            }
            if (q_max != -1)
            {
SelectedMax.Add(qi_max);
            }
            return Selected;
```

```
        }

        public static List<int>SearchOptimalAtFourth()
        {
inti, qi_max = -1;
            double q_max = 0, v_min = 99999;
SelectedMax.Clear();
Selected.Clear();

            for (i = 0; i<Q.Count(); i++)
            {
                if (Q[i] <= q_por&& V[i] >= V_por)
                {
Selected.Add(i);
                }
            }
            for (i = 0; i<Q.Count(); i++)
            {
                if (Q[i] <= q_por&& V[i] >= V_por&& Q[i] >q_max)
                {
q_max = Q[i];
qi_max = i;
                }
            }
            if (qi_max != -1)
            {
SelectedMax.Add(qi_max);
}

returnSelected;
        }
    }
}
```

ҚОСЫМША Ә

«ЖОО АББО киберқауіпсіздігін қамтамасыз ету үшін рационалды қаржы стратегияларын таңдау» ШҚҚЖ бағдарламалық өнімінің коды

Form 1

```
using System;
using System.IO;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading;
using System.Threading.Tasks;
using System.Windows.Forms;
using Microsoft.Win32;
// This is the code for your desktop app.
// Press Ctrl+F5 (or go to Debug > Start Without Debugging) to run your app.
namespace DesktopApp2
{
   public partial class Form1 : Form
   {
      private double kd ,h, q , g1, g2, f1, f2, m1 , m2, p1 ,p2;//задаваемые данные
      Gamers G1, G2;//игроки, связываем классы композицией
      int maxStep = 25;
      private void button1_Click(object sender, EventArgs e)
      {
         int i = 0;
         double k = 0;
         double kLast = 0;
         double qChanged = q / kd;
         //игроки
         G1 = new Gamers(kd, h, g1, f1, m1, p1, 1);
         G2 = new Gamers(kd, q, g2, f2, m2, p2, 2);
         if ((G1.GetZ() >= 0 && G2.GetZ() >= 0))//случай а
         {
            double z1 = G1.GetZ();
            double z2 = G2.GetZ();
            //MessageBox.Show("z1 = " + Convert.ToString(z1) + " " + "z2 = " +Convert.ToString(z2));
            if (g1 > g2)
            {
               bool permission = false;
               while (i <= maxStep)
               {
                  Thread.Sleep(1);
                  if (i == 0)
                  {
                     k = 0;
                  }//k(0) = 0
```

```
                else
                {
                    k = (g1 / g2) * ((z1 + z1 * kLast + kLast * kd) / (1 + z2 + (z2 / kd) * kLast));
                }
                if (k > z1 / z2 && kLast <= z1 / z2)
                {
                    //достигнуто максимальное количество шагов
                    permission = true;
                    break;
                }
                kLast = k;
                i++;
            }
            if (permission == true)
            {
                int step;
                bool LocalPermission = false;
                for (step = 1; step <= i+1; step++)
                {
                    if (kLast * h <= q && q < k * h)
                    {
                        LocalPermission = true;
                        G1.SetUV(1);
                        G2.SetUV(1);
                        Form3 form3 = new Form3(G1, G2, step+2, GetWay(), "a1");
                        form3.Show();
                        break;
                    }
                }
                if(!LocalPermission)
                {
                    Form7 form = new Form7("Ресурсы 2-го игрока не принадлежат множеству
предпочтительности!");
                    form.Show();
                }
            }
            else
            {
                Form7 form = new Form7("Невозможно построить график!");
                form.Show();
            }
        }//подслучай a1
        else if (g1 <= g2)
        {
            double z = 0;
            //для уравнений
            double x1, x2;
            double a, b, c; //коэфициенты для квадратного уравнения
            a = G2.GetZ();
            b = 1 - G2.GetZ() - (g1 / g2) * G1.GetZ() - (g1 / g2);
            c = -(g1 / g2) * G1.GetZ();
            //квадратное уравнение
            double Y1 = -b + Math.Sqrt(Math.Pow(b, 2) - 4 * a * c);//x1
```

```
double Y2 = -b - Math.Sqrt(Math.Pow(b, 2) - 4 * a * c);//x2
x1 = Y1 / (2 * a);
x2 = Y2 / (2 * a);
if (0 < x2)
{
   z = x2;
}
else if (0 < x1)
{
   z = x1;
}
else if(x1 < x2)
{
   z = x1;
}
else if(x2 < x1)
{
   z = x2;
}

//*****************************************************************
//MessageBox.Show(Convert.ToString(z * h));
if (q < z * h)//основное условие
{
   while (true)
   {
      Thread.Sleep(1);
      if (i <= maxStep)
      {
      if (i == 0)
         {
            k = 0;
         }
         else
         {
            k = (g1 / g2) * ((z1 + z1 * kLast + kLast * kd) / (1 + z2 + (z2 / kd) * kLast));
            //MessageBox.Show(Convert.ToString(k) + " " + Convert.ToString(k * h));
         }
         if (kLast * h <= q && q < k * h)
         {
            G1.SetUV(1);
            G2.SetUV(1);
            Form3 form3 = new Form3(G1, G2, i + 1, GetWay(), "a2");
            form3.Show();
            break;
         }
      }
      else
      {
         Form7 form = new Form7("Количество шагов слишком большое для вывода графика!");
         form.Show();
         break;
      }
```

```
                    i++;
                    kLast = k;
                }
            }
            else if(q == z * h)
            {
                G1.SetUV(1);
                G2.SetUV(1);
                Form3 form3 = new Form3(G1, G2, maxStep, GetWay(), "a2");
                form3.Show();
            }
            else
            {
                Form7 form = new Form7("Точка находится в области предпочтительности 2-го игрока!");
                form.Show();
            }
        }//подслучай a2
    }//случай a
    else if (G1.GetZ() < 0 && G2.GetZ() < 0)
    {
        Form7 form = new Form7("Любые состояния игроков являются для них предпочтительными, а
оптимальными стратегиями являются их любые стратегии.");
        form.Show();
    }//случай b
    else if ((G1.GetZ() > 0 && G2.GetZ() <= 0))
    {
        double z1 = G1.GetZ();
        double z2 = G2.GetZ();

        if ((g1 / g2) * (z1 + 1) >= 1)
        {
            Form7 form = new Form7("Множеством предпочтительности первого игрока являются все
начальные финансовые ресурсы игроков.");
            form.Show();
        }//подслучай c1
        else if ((g1 / g2) * (z1 + 1) < 1)
        {
            double z = (g1 / g2) * z1 * kd / (1 - (z1 + 1) * (g1 / g2));
            if (q < z * h)
            {
                while (i <= maxStep)
                {
                    Thread.Sleep(1);
                    if(i == 0)
                    {
                        k = 0;
                    }
                    else
                    {
                        k = (g1 / g2) * (z1 * kd + z1 * kLast + kLast);
                    }
                    if (kLast * h <= q && q < k * h)
                    {
```

```
                    G1.SetUV(1);
                    G2.SetUV(0);
                    Form3 form3 = new Form3(G1, G2, i+1, GetWay(), "c2");
                    form3.Show();
                    break;
                }
                kLast = k;
                i++;
            }
            if (i > maxStep)
            {
                Form7 form = new Form7("Количество шагов слишком большое для вывода графика!");
                form.Show();
            }
        }
        else
        {
            Form7 form = new Form7("Ресурсы не принадлежат множеству предпочтительности!");
            form.Show();
        }
      }//подслучай c2
    }//случай c
    else if (G1.GetZ() <= 0 && G2.GetZ() > 0)
    {
      Form7 form = new Form7("Первый игрок не может в этом случае иметь свое множество
предпочтительности.");
      form.Show();
    }//случай d
  }
  //*********************************************************************
  private void textBox10_TextChanged(object sender, EventArgs e)
  {
    try
    {
      if (Convert.ToDouble(textBox10.Text) <= 9999999999999)
      {
        textBox10.ForeColor = Color.Black;//меняем цвет шрифта обратно
        p2 = Convert.ToDouble(textBox10.Text);
      }
      else
      {
        textBox10.ForeColor = Color.Gray;//меняем цвет шрифта обратно
      }
    }
    catch (System.FormatException)
    {
      textBox10.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
  }
  private void textBox9_TextChanged(object sender, EventArgs e)
  {
    try
    {
```

```
        if (Convert.ToDouble(textBox9.Text) <= 9999999999999)
        {
            textBox9.ForeColor = Color.Black;//меняем цвет шрифта обратно
            p1 = Convert.ToDouble(textBox9.Text);
        }
        else
        {
            textBox9.ForeColor = Color.Gray;//меняем цвет шрифта обратно
        }
    }
    catch (System.FormatException)
    {
        textBox9.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}
private void textBox8_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (Convert.ToDouble(textBox8.Text) <= 9999999999999)
        {
            textBox8.ForeColor = Color.Black;//меняем цвет шрифта обратно
            m2 = Convert.ToDouble(textBox8.Text);
        }
        else
        {
            textBox8.ForeColor = Color.Gray;//меняем цвет шрифта обратно
        }
    }
    catch (System.FormatException)
    {
        textBox8.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}
private void textBox4_MouseMove(object sender, MouseEventArgs e)
{
    label8.ForeColor = Color.LightBlue;
}
private void textBox4_MouseLeave(object sender, EventArgs e)
{
    label8.ForeColor = Color.White;
}
private void button1_MouseMove(object sender, MouseEventArgs e)
{
    button1.ForeColor = Color.LightBlue;
    button1.BackColor = Color.Gray;
    button1.FlatAppearance.BorderColor = Color.Gray;
    panel3.BackColor = Color.LightBlue;
}
private void button1_MouseLeave(object sender, EventArgs e)
{
    button1.BackColor = Color.FromArgb(64, 64, 64);
    button1.FlatAppearance.BorderColor = Color.FromArgb(64, 64, 64);
```

```
    button1.ForeColor = Color.White;
    panel3.BackColor = Color.FromArgb(64,64,64);
}
private void textBox7_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (Convert.ToDouble(textBox7.Text) <= 9999999999999)
        {
            textBox7.ForeColor = Color.Black;//меняем цвет шрифта обратно
            m1 = Convert.ToDouble(textBox7.Text);
        }
        else
        {
            textBox7.ForeColor = Color.Gray;//меняем цвет шрифта обратно
        }
    }
    catch (System.FormatException)
    {
        textBox7.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}
private void textBox6_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (Convert.ToDouble(textBox6.Text) <= 9999999999999)
        {
            textBox6.ForeColor = Color.Black;//меняем цвет шрифта обратно
            f2 = Convert.ToDouble(textBox6.Text);
        }
        else
        {
            textBox6.ForeColor = Color.Gray;//меняем цвет шрифта обратно
        }
    }
    catch (System.FormatException)
    {
        textBox6.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}
private void textBox5_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (Convert.ToDouble(textBox5.Text) <= 9999999999999)
        {
            textBox5.ForeColor = Color.Black;//меняем цвет шрифта обратно
            f1 = Convert.ToDouble(textBox5.Text);
        }
        else
        {
            textBox5.ForeColor = Color.Gray;//меняем цвет шрифта обратно
```

```
        }
    }
    catch (System.FormatException)
    {
        textBox5.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}
private void textBox4_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (Convert.ToDouble(textBox4.Text) <= 9999999999999)
        {
            textBox4.ForeColor = Color.Black;//меняем цвет шрифта обратно
            g2 = Convert.ToDouble(textBox4.Text);
        }
        else
        {
            textBox4.ForeColor = Color.Gray;//меняем цвет шрифта обратно
        }
    }
    catch (System.FormatException)
    {
        textBox4.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}
private void textBox3_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (Convert.ToDouble(textBox3.Text) <= 9999999999999)
        {
            textBox3.ForeColor = Color.Black;//меняем цвет шрифта обратно
            g1 = Convert.ToDouble(textBox3.Text);
        }
        else
        {
            textBox3.ForeColor = Color.Gray;//меняем цвет шрифта обратно
        }
    }
    catch (System.FormatException)
    {
        textBox3.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}

private void button2_Click(object sender, EventArgs e)
{
    Form5 setting = new Form5();
    setting.Location = new Point(Location.X  + 241, Location.Y);
    setting.Show();
}
```

```
private void textBox11_TextChanged(object sender, EventArgs e)
{

   try
   {
      if (Convert.ToDouble(textBox11.Text) <= 9999999999999)
      {
         textBox11.ForeColor = Color.Black;//меняем цвет шрифта обратно
         kd = Convert.ToDouble(textBox11.Text);
      }
      else
      {
         textBox11.ForeColor = Color.Gray;//меняем цвет шрифта обратно
      }
   }
   catch (System.FormatException)
   {
      textBox11.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
   }
}
private void textBox2_TextChanged(object sender, EventArgs e)
{
   try
   {
      if (Convert.ToDouble(textBox2.Text) <= 9999999999999)
      {
         textBox2.ForeColor = Color.Black;//меняем цвет шрифта обратно
         q = Convert.ToDouble(textBox2.Text);
      }
      else
      {
         textBox2.ForeColor = Color.Gray;//меняем цвет шрифта обратно
      }
   }
   catch (System.FormatException)
   {
      textBox2.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
   }
}
private void textBox1_TextChanged(object sender, EventArgs e)
{

   try
   {

     if (Convert.ToDouble(textBox1.Text) <= 9999999999999)
     {
         textBox1.ForeColor = Color.Black;//меняем цвет шрифта обратно
         h = Convert.ToDouble(textBox1.Text);
     }
     else
     {
       textBox1.ForeColor = Color.Gray;//меняем цвет шрифта обратно
```

```
      }
    }
    catch(System.FormatException)
    {
      textBox1.ForeColor = Color.Red;//меняем цвет шрифта, если ловим исключение
    }
}
////////////////////////////////////////////////////////////////////////////////////
private void textBox_DoubleClick(object sender, EventArgs e)
{
    var textBox = sender as TextBox;
    textBox.SelectAll();
    textBox.Focus();
}
private void textBox_Click_Left(object sender, EventArgs e)
{
    label7.ForeColor = Color.LightBlue;
    label6.ForeColor = Color.White;
}
private void textBox_Click_Right(object sender, EventArgs e)
{
    label6.ForeColor = Color.LightBlue;
    label7.ForeColor = Color.White;
}
private void textBox4_Click(object sender, EventArgs e)
{
    label7.ForeColor = Color.White;
    label6.ForeColor = Color.White;
}
private void textBox_MouseMove(object sender, MouseEventArgs e)
{
    var textBox = sender as TextBox;
    textBox.BackColor = Color.LightBlue;
}
private void textBox_MouseLeave(object sender, EventArgs e)
{
    var textBox = sender as TextBox;
    textBox.BackColor = Color.White;
}
////////////////////////////////////////////////////////////////////////////////////
public Form1()
{
    InitializeComponent();

}
private string GetWay()
{
    //создаем директорию для хранения скриншотов
    //записываем в нее файл с коэффициентами
    //и передаем путь в следующую форму
    //где в эту директорию будет сохранен скриншот

    string path = null;
```

```
        string way = null;
        try
        {

            RegistryKey currentUser = Registry.CurrentUser;
            RegistryKey saves = currentUser.OpenSubKey("Saves");
            path = saves.GetValue("ScreenWay").ToString();
            way = path + "\\" + "time " + Convert.ToString(DateTime.Now.ToString("hh.mm.ss"));//путь для
хранения графика, значений и таблицы
            saves.Close();
        }
        catch
        {
            RegistryKey currentUser = Registry.CurrentUser;
            RegistryKey saves = currentUser.CreateSubKey("Saves");//если нет, то создаем его
            saves.SetValue("ScreenWay", "C:\\Screens");//папка для скриншотов по умолчанию

            path = saves.GetValue("ScreenWay").ToString();
            way = path + "\\" + "time " + Convert.ToString(DateTime.Now.ToString("hh.mm.ss"));//путь для
хранения графика, значений и таблицы
            saves.Close();
        }
        Directory.CreateDirectory(way);

/**********************************************************************************************
****************
        StreamWriter writer = new StreamWriter(way + "\\" + "coefficients.txt", false,
System.Text.Encoding.Default);
        writer.WriteLine("СЛЕВА 1-ЫЙ ИГРОК , СПРАВА 2-ОЙ ИГРОК");

writer.WriteLine("**********************************************************************************
**************");
        writer.WriteLine("                        Курс валют: " + kd);
        writer.WriteLine("                          Ресурсы: " + h + "    " + q);
        writer.WriteLine("                        Темп роста: " + g1 + "    " + g2);
        writer.WriteLine("         Доля на погашение задолжености: " + f1 + "    " + f2);
        writer.WriteLine(" Процентная ставка по выделяемым ресурсам: " + m1 + "    " + m2);
        writer.WriteLine("Доля возвращаемых инвестиционных ресурсов: " + p1 + "    " + p2);

writer.WriteLine("**********************************************************************************
**************");
        writer.Close();

//**********************************************************************************************
*****************
        return way;//возвращаем папку для хранения информации
    }

    private void Form1_Load(object sender, EventArgs e)
    {
        //создаем ключи в реестре
        try
        {
```

```
            RegistryKey currentUser = Registry.CurrentUser;
            RegistryKey saves = currentUser.OpenSubKey("Saves", true);//проверяем, существует ли ключ в
реестре
            saves.Close();
         }
         catch
         {
            RegistryKey currentUser = Registry.CurrentUser;
            RegistryKey saves = currentUser.CreateSubKey("Saves");//если нет, то создаем его
            saves.SetValue("ScreenWay", "C:\\Screens");//папка для скриншотов по умолчанию
            saves.Close();
         }
      }
   }
}
```

Form 3

```
using System;
using System.IO;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Windows.Forms.DataVisualization.Charting;
using Microsoft.Win32;
namespace DesktopApp2
{
   public partial class Form3 : Form
   {
      private string way;
      private bool increase = false;

      //public Panel panel1;
      public Form3()
      {
         InitializeComponent();
      }
      public Form3(Gamers G1, Gamers G2, int x, string way, string Case)
      {
         double LastY = G2.GetMoney();
         this.way = way;//путь для хранения скриншота графика
         Form4 form4 = new Form4();//таблица значений
         form4.SetColums();
         Chart chart1 = new Chart();
         chart1.MaximumSize = new Size(816, 460);
         chart1.Visible = false;
         //chart1.Click += new EventHandler();
         chart1.Parent = this;
         chart1.Dock = DockStyle.Fill;
```

```
chart1.ChartAreas.Add(new ChartArea("Math function"));
//создаем набор точек
Series series = new Series();
series.Color = Color.Aqua;
series.BorderWidth = 3;
series.ChartType = SeriesChartType.Line;
series.MarkerStyle = MarkerStyle.Circle;
for (int i = 0; i < x; i++)
{
   if (G2.GetMoney() > 0)
   {
      series.Points.AddXY(G1.GetMoney(), G2.GetMoney());
      form4.SetTable(i, G1.GetMoney(), G2.GetMoney());
      G1.Equation(G2);
      G2.Equation(G1);
   }
   else
   {
      series.Points.AddXY(G1.GetMoney(), G2.GetMoney());
      form4.SetTable(i, G1.GetMoney(), G2.GetMoney());
      break;
   }
   //заполнение комментария к графику
   if (LastY < G2.GetMoney())
   {
      increase = true;
   }
   LastY = G2.GetMoney();
}
      //chart1.ChartAreas[0].AxisX.LineColor = Color.Red;
////////////////////////////////////////////////
//настройка chart1
chart1.ChartAreas[0].AxisX.LabelStyle.Format = "{0:0,}K";
chart1.ChartAreas[0].AxisY.LabelStyle.Format = "{0:0,}K";
chart1.BackColor = Color.FromArgb(64, 64, 64);
chart1.ChartAreas[0].BackColor = Color.FromArgb(99, 99, 99);
chart1.ChartAreas[0].AxisX.MajorGrid.LineColor = Color.LightBlue;
chart1.ChartAreas[0].AxisY.MajorGrid.LineColor = Color.LightBlue;
chart1.ChartAreas[0].AxisX.LabelStyle.ForeColor = Color.White;
chart1.ChartAreas[0].AxisY.LabelStyle.ForeColor = Color.White;

////////////////////////////////////////////////
series.Points[0].MarkerStyle = MarkerStyle.Circle;
series.Points[0].MarkerSize = 11;
series.Points[0].MarkerColor = Color.Red;

//chart1.ChartAreas[0].AxisY.Minimum = 0;
chart1.Series.Add(series);
//*************************************************************************
//делаем скриншот графика
int width = chart1.Width;
int heigth = chart1.Height;
chart1.Width = 1280;
```

```
            chart1.Height = 720;
            way += "\\screen.png";
            try
            {
                chart1.SaveImage(way, System.Drawing.Imaging.ImageFormat.Png);
            }
            catch
            {
                Form7 form = new Form7("Директория для хранения скриншотов недоступна! Смените путь в
настройках!");
            }
            chart1.Width = width;
            chart1.Height = heigth;
            chart1.Visible = true;
           //*************************************************************************
            TextBox textBox1 = new TextBox();
            textBox1.Multiline = true;
            textBox1.Location = new Point(0, 460);
            textBox1.Size = new Size(800, 101);
            textBox1.ReadOnly = true;
            textBox1.Font = new Font("Century Gothic", 12, FontStyle.Regular);
            textBox1.ForeColor = Color.FromArgb(64, 64, 64);
            if (!increase)
            {
                textBox1.Text = "В данном случае, первый игрок, применяя свою оптимальную стратегию,
добивается цели во взаимодействии. Это означает, что второй игрок потеряет свой финансовый ресурс,
несмотря на его противодействие первому игроку.";
            }
            else
            {
                textBox1.Font = new Font("Century Gothic", 10, FontStyle.Regular);
                textBox1.Text = "В этом случае, первый игрок (защитник ИОСУ), применяя свою оптимальную
стратегию, добивается своей цели во взаимодействии, т.е. приводит второго игрока (Хакера) к потере
финансового ресурса, несмотря на его оптимальное противодействие. При этом преимущество второго
игрока в темпе роста дало ему возможность оказать первому игроку серьезное противодействие, что
позволило ему даже нарастить свою величину финансового ресурса на некотором промежутке времени.
";
            }
            //*************************************************************************
            textBox1.SendToBack();
            this.Controls.Add(textBox1);
            form4.Show();
            InitializeComponent();

        }
        private void Form3_Load(object sender, EventArgs e)
        {
            //panel1 = new Panel();
            //panel1.BackColor = Color.Red;

        }
    }
}
```

Form 5

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using Microsoft.Win32;
namespace DesktopApp2
{
   public partial class Form5 : Form
   {
      private string way;
      public string GetWay()
      {
         return way;
      }
      public Form5()
      {
         InitializeComponent();
         try
         {
            RegistryKey currentUser = Registry.CurrentUser;
            RegistryKey saves = currentUser.OpenSubKey("Saves");
            way = saves.GetValue("ScreenWay").ToString();
            saves.Close();
         }
         catch//если в реестре отсутствует ключ
         {
            RegistryKey currentUser = Registry.CurrentUser;
            RegistryKey saves = currentUser.CreateSubKey("Saves");//если нет, то создаем его
            saves.SetValue("ScreenWay", "C:\\Screens");
            way = saves.GetValue("ScreenWay").ToString();
            saves.Close();
         }
         label3.Text = way;
      }
      private void panel1_MouseMove(object sender, MouseEventArgs e)
      {
         label1.BackColor = Color.FromArgb(99, 99, 99);
         panel1.BackColor = Color.FromArgb(99, 99, 99);
         label1.ForeColor = Color.LightBlue;
         panel3.BackColor = Color.LightBlue;
      }
      private void panel1_MouseLeave(object sender, EventArgs e)
      {
         label1.BackColor = Color.FromArgb(64, 64, 64);
         panel1.BackColor = Color.FromArgb(64, 64, 64);
         label1.ForeColor = Color.White;
         panel3.BackColor = Color.FromArgb(64, 64, 64);
```

```
}
private void panel2_MouseMove(object sender, MouseEventArgs e)
{
   panel2.BackColor = Color.FromArgb(99, 99, 99);
   label2.BackColor = Color.FromArgb(99, 99, 99);
   label2.ForeColor = Color.LightBlue;
   panel4.BackColor = Color.LightBlue;
}
private void panel2_MouseLeave(object sender, EventArgs e)
{
   panel2.BackColor = Color.FromArgb(64, 64, 64);
   label2.BackColor = Color.FromArgb(64, 64, 64);
   label2.ForeColor = Color.White;
   panel4.BackColor = Color.FromArgb(64, 64, 64);
}

private void panel2_Click(object sender, EventArgs e)
{
   FolderBrowserDialog folder = new FolderBrowserDialog();
   folder.Description = "Выбор директории для хранения скриншотов графиков";
   folder.SelectedPath = @"C:\";
   if (folder.ShowDialog() == DialogResult.OK)
   {
      way = folder.SelectedPath;
      try
      {
         RegistryKey currentUser = Registry.CurrentUser;
         RegistryKey saves = currentUser.OpenSubKey("Saves", true);
         saves.SetValue("ScreenWay", way);
         saves.Close();
      }
      catch//если в реестре отсутствует ключ
      {
         RegistryKey currentUser = Registry.CurrentUser;
         RegistryKey saves = currentUser.CreateSubKey("Saves");
         saves.SetValue("ScreenWay", way);
         saves.Close();
      }
      label3.Text = way;
      //MessageBox.Show(folder.SelectedPath);
   }
}
private void label1_Click(object sender, EventArgs e)
{
}
private void linkLabel1_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
{
```

MessageBox.Show("Программа основана на математической модели для нахождения стратегий управления инвестированием в средства информационной и кибербезопасности ИОС университета. Программа концептуально построена на решении билинейной динамической игры качества с несколькими терминальными поверхностями, а ее отличительной чертой является тот факт, что дискретные уравнения, задающие динамику игры, записаны с помощью произвольных

```
коэффициентов.\n\n" + "Авторы: Лахно В., Ахметов Б., Кыдыралина Л.", "О программе", MessageBoxButtons.OK, MessageBoxIcon.Question);
        }
    }
}
```

Form Gamers

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
namespace DesktopApp2
{
    public class Gamers : Form3
    {
        protected double kd, money, g, f, m, p;
        protected double uv;
        protected int priority;
        protected double last_money;
        public Gamers( double kd, double money, double g, double f, double m, double p, int priority)
        {
            this.kd = kd;
            this.money = money;
            this.g = g;
            this.f = f;
            this.m = m;
            this.p = p;
            uv = 0;
            this.priority = priority;
        }
        public void SetUV(double uv)
        {
            this.uv = uv;
        }
        public double GetZ()
        {
            double z = (1 - f) * (m + p) - 1;
            return z;
        }
        public double GetUV()
        {
            return uv;
        }
        public double GetMoney()
        {
            return money;
        }
        public double GetLastMoney()
        {
            return last_money;
        }
```

```
        public void Equation(Gamers gamer)
        {
            last_money = money;
            if (priority == 1)
            {
                // MessageBox.Show(Convert.ToString(g * money) + " + " + Convert.ToString((1 - f) * (m + p) - 1) +
" * " + Convert.ToString(uv) + " * " + Convert.ToString(g * money) + " + " + Convert.ToString(1 - (gamer.m +
gamer.p) * (1 - gamer.f)) + " * " + Convert.ToString(gamer.uv + " * " + gamer.g + " * " + gamer.money / kd));
                money = g * money + ((1 - f) * (m + p) - 1) * uv * g * money + (1 - (gamer.m + gamer.p) * (1 -
gamer.f)) * gamer.uv * gamer.g * gamer.money / kd;
            }
            else if(priority == 2)
            {
                // MessageBox.Show(Convert.ToString(g * money) + " + " + Convert.ToString((1 - f) * (m + p) - 1) +
" * " + Convert.ToString(uv) + " * " + Convert.ToString(g * money) + " + " + Convert.ToString(1 - (gamer.m +
gamer.p) * (1 - gamer.f)) + " * " + Convert.ToString(gamer.uv + " * " + gamer.g + " * " + gamer.last_money *
kd));
                money = g * money + ((1 - f) * (m + p) - 1) * uv * g * money + (1 - (gamer.m + gamer.p) * (1 -
gamer.f)) * gamer.uv * gamer.g * gamer.last_money * kd;
            }
        }
    }
}
```

ҚОСЫМША Б

Оқу процесіне енгізу туралы актілері

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

03041, м. Київ, вул. Героїв Оборони, 16, навчальний корпус № 15, тел./факс: (044) 527-83-52,
E-mail: o-glazunova@nubip.edu.ua

018 № 16-35
На № _____ від 12.03.2020 р.

Акт
о внедрении результатов диссертационной работы
Кыдыралины Лазат Муктаровны

Комиссия в составе:

председатель – декан факультета информационных технологий Национального университета биоресурсов и природопользования Украины (НУБИП), д.пед.н. проф. Глазунова Е.Г.

члены комиссии: д.т.н., проф. Лахно В.А., д.ф.-м.н., проф. Малюкова В.П.

составила настоящий акт, о том, что результаты теоретических и экспериментальных исследований, проведенных в рамках диссертационной работы Кыдыралины Лазат Муктаровны «Методы и модели интегрированной защиты информационной образовательной среды вуза», позволили апробировать и внедрить в учебном процессе факультета ИТ НУБИП Украины следующие результаты:

1) Методика оперативного управления кибербезопасностью информационно-коммуникационных систем университета на основе комплексной интеграции систем поддержки принятия решений (СППР) по информационной безопасности;
2) СППР для выбора рациональных финансовых стратегий для формирования контуров кибербезопасности информационной образовательной среды вуза.

Председатель:
Декан факультета
информационных технологий — д.пед.н., проф. Глазунова Е.Г.

Члены комиссии: д.т.н., проф. Лахно В.А.
д.ф.-м.н., проф. Малюков В.П.

Qazaqstan Respýblıkasy
Bilim jáne ǵylym mınıstrligi

**«Semeı qalasynyń
Shákárim atyndaǵy ýnıversıteti»
komersıalyq emes
akcıonerlik qoǵam**

QR, 071412, ShQO, Semeı q., Glınki kósh., 20a,
e-mail: semgu@bk.ru, 8 (7222) 32-35-13
BIN 130840007973, KBe 16, BIK HSBKKZKX
KUJK KODY 30958953, EQTJK 85421, TMK 861
IIK KZ126010261000182423, AQ «Qazaqstan Halyq Banki»

10.08.2020 № 455

№

Министерство образования и науки
Республики Казахстан

**Некоммерческое
акционерное общество
«Университет имени Шакарима
города Семей»**

РК, 071412, ВКО, г.Семей, ул.Глинки, 20а,
e-mail: semgu@bk.ru, 8 (7222) 32-35-13
БИН 130840007973, КБе 16, БИК HSBKKZKX
КОД ОКПО 30958953, ОКЭД 85421, КНП 861
ИИК KZ126010261000182423, в АО «Народный Банк Казахстана»

Кыдыралина Лазат Муктаровнаның диссертациялық жұмысының нәтижелерін оқу процесіне енгізу туралы

АКТ

Біз төменде қол қоюшылар «Шәкәрім атындағы университеті» КЕ АҚ, «Білім алуды жалғастыру» факультетінің деканы, т.ғ.д., профессор А.К.Какимов, «Ақпараттық-коммуникациялық технологиялар» факультетінің деканы, философия ғылымдарының докторы (PhD) А.К. Шайханова, «Автоматтандыру және ақпараттық технологиялар» кафедрасының меңгерушісі, т.ғ.к. А.Д. Золотов болып, Қыдыралина Лазат Муктаровнаның 6D060200 – Информатика мамандығы бойынша философия ғылымдарының докторы (PhD) дәрежесін алу үшін дайындаған «Жоғары оқу орнының ақпараттық білім беру ортасын интеграцияланған қорғаудың әдістері мен модельдері» тақырыбындағы диссертациясының теориялық және эксперименттік зерттеулерінің нәтижелерін «Шәкәрім атындағы университеті» КЕ АҚ, «Ақпараттық-коммуникациялық технологиялар» факультетінің оқу процесінде, атап айтсақ 7М06102 – «Информатика» мамандығының, 1 курс магистранттары үшін онлайн курста пайдаланғандығын растап қол қоямыз.

Ректор м.а. _____ У.Б.Тлемисов

«Білім алуды жалғастыру» факультетінің деканы, т.ғ.д., профессор _____ А.К.Какимов

«Ақпараттық-коммуникациялық технологиялар» факультетінің деканы, философия ғылымдарының докторы _____ А.К. Шайханова

«Автоматтандыру және ақпараттық технологиялар» кафедрасының меңгерушісі, т.ғ.к. _____ А.Д. Золотов

«Kaspersky LAB KZ» ЖШС
Қазақстан, 050010, Алматы қаласы,
Қазыбек би көшесі, 20А
офис 309

+7 727 225 11 51
sales@kz.kaspersky.com
www.kaspersky.ru

ТОО «Kaspersky LAB KZ»
Республика Казахстан, 050010
г. Алматы, ул. Казыбек би, 20 А
офис 309

+7 727 225 11 51
sales@kz.kaspersky.com
www.kaspersky.ru

АКТ
внедрения результатов диссертационной работы
Кыдыралиной Лазат Муктаровны

на тему «Методы и модели интегрированной защиты информационной образовательной среды вуза».

1. Разработаны и протестированы алгоритмы оптимального выбора при проектировании технических средств охраны (ТСО) и средств защиты информации СЗИ для информационной образовательной среды (ИОС) вуза с учетом всех возможных вариантов реализации системы информационной и кибербезопасности.

3. Разработана компьютерная программа «Модуль СППР IDSS (Метод Парето для выбора СЗИ)», реализующая алгоритмы оптимального выбора при проектировании ТСО и СЗИ для ИОС вуза.

4. Разработан программный продукт, основанный на применении нового класса билинейных дифференциальных игр. Данный класс позволил адекватно описать процесс и отыскать оптимальные стратегии финансирования стороной защиты средств кибербезопасности ИОС вуза. Разработан модуль в среде программирования VisualStudio 2017 для системы поддержки решений – «Выбор рациональной финансовой стратегии для обеспечения кибербезопасности ИОС вуза (IDSS)». В модуле «IDSS» реализована предложенная модель, базирующаяся на применении методов теории дифференциальных игр. Разработанный модуль, позволяет уменьшить расхождения данных прогнозирования и реальной отдачи от инвестирования в средства защиты информации и кибербезопасности ИОС вуза. Решение позволяет получить оптимальные стратегии финансирования стороной защиты средств кибербезопасности для ИОС вуза. Программная реализация модуля СППР позволяет выбрать оптимальную финансовую составляющую стратегии стороны защиты при любых соотношениях параметров, описывающих процесс финансирования, как бы финансово не действовала вторая сторона, пытающаяся взломать периметры защиты ИОС вуза.

10.02.2020

С уважением,

Питолин Е.В.
Управляющий директор
в Центральной Азии, странах СНГ и Балтии

Справка

выдана докторанту по специальности 6D060200 – «Информатика» Кыдыралиной Лазат Муктаровне в том, что она действительно была исполнителем совместного проекта КазНПУим.Абая с НИИ Высшая Школа Экономики (Россия, г.Москва) по теме «Мониторинг проникновения цифровых инструментов в учебный процесс вуза» (договор НИР № 19/04 от 19.04.2019).

и.о. директора
Департамента науки
д.п.н., профессор У.М.Абдигапбарова