Қыдыралина Лазат Муктаровнаның
6D060200 – «Информатика» мамандығы бойынша философия докторы (PhD) дәрежесін алу үшін ұсынған «Жоғары оқу орнының ақпараттық білім беру ортасын кіріктірілген қорғаудың әдістері мен модельдері» тақырыбындағы диссертациясына

АҢДАТПА

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.

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.

Қаскүнемдер (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, С.В. Казмирчук, В.А.Лахно, А.Г.Корченко, В.И.Котенко, M.Atighetchi, R.H.Campbell, J. Dawkins, А.С. Марков, M.Endler айналысқан. Бұл мәселелерді зерттеуге отандық мамандар да өз үлестерін қосты: Р.Г.Бияшев, М.Н.Калимолдаев, Б.С. Ахметов, У.А.Тукеев, И.Т.Утепбергенов, В.В.Яворский, Т.С.Картбаев, Ж.К.Алимсеитова 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: VisualStudio2017 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.

АННОТАЦИЯ
диссертационной работы Кыдыралиной Лазат Муктаровны
«Методы и модели интегрированной защиты информационной образовательной среды вуза», представленной на соискание степени доктора философии (PhD)
по специальности 6D060200 – Информатика

Актуальность исследования: Ключевую роль в области развития и повышения эффективности деятельности вузов играет его ориентация на постоянный поиск и применение новейших подходов, технологий и средств, появляющихся в мире по мере развития науки и техники. В связи с этим вузы не могут оставаться в стороне от глобальных процессов цифровизации и информатизации, особенно актуальных в последние годы в связи с выделением и формированием новых видов технологий и средств, относимых к четвёртой индустриальной революции. Такие технологии позволяют техническим средствам взаимодействовать друг с другом без участия человека. Дополнительным стимулом для развития образовательных систем является формирование новых поколений людей, готовых и способных жить и учиться, повсеместно используя цифровые технологии.

С учётом этих и других факторов своевременная комплексная и всеобъемлющая цифровизация приобретает стратегический характер, требует поиска и систематизации соответствующих концептуальных подходов. Ярким примером этому служит концепция цифровизации Казахского национального педагогического университета имени Абая, разработанная под руководством профессора Т.О.Балыкбаева и профессора Е.Ы.Бидайбекова. Концепция нацелена на обеспечение целостности и долгосрочного планомерного развития подходов к интеграции и использованию цифровых технологий и средств для повышения эффективности всех видов деятельности КазНПУ им. Абая как цифрового университета. Содержание концепции сформировано с учётом результатов анализа цифровой инфраструктуры университета, на основе которого определены приоритетные направления цифровизации университета. Рассматриваются теоретические и практические основы цифровизации образовательной и учебно-методической деятельности, научных исследований и интеграции университета в мировое научное сообщество, подходы к развитию цифровой компетентности студентов и преподавателей в условиях цифровизации университета.

В Концепции особое внимание уделяется вопросам информационной безопасности (ИБ) и ее составляющей кибербезопасности (КБ) цифровой образовательной среды университета. В современных вузах трудится большое количество педагогов, научных сотрудников, обучаются десятки тысяч студентов, составляющих интеллектуальный и трудовой потенциал развития любого государства. В связи с чем задача обеспечения ИБ и КБ вузов и других учебных заведений в современных условиях имеет огромное значение.

Следует отметить, что в области обеспечения ИБ и управления КБ вузов существует целый ряд проблем, среди которых наиболее существенными являются: слабая оснащенность ИОС вузов средствами технической защиты информационных ресурсов (СТЗИ); имеющийся моральный и физический износ оборудования, обеспечивающего решения задач по обеспечению КБ (коммутаторов, маршрутизаторов, файерволов и др.); отсутствие в штатных расписаниях IT департаментов вузов специально подготовленных специалистов, ответственных именно за вопросы ИБ и КБ вуза, которые могли бы грамотно и оптимально распределять целевое финансирование, которое выделяется на обеспечение КБ ИОС вузов.

Существующие подходы к управлению КБ ИОС вузов в основном базируются на решениях, которые характерны в основном для коммерческих предприятий или так называемых режимных объектов. Однако образовательные учреждения и вузы, в частности, обладают собственной спецификой. Проектировщики систем КБ ИОС вузов отмечают следующие трудности в процессе построения систем управления ИБ:

– с отсутствием специальных методик и методов оценки текущего состояния ИБ и КБ вуза;

– с неопределенностью и специфичностью дестабилизирующих факторов, которые могут воздействовать на защищаемые ресурсы ИОС вуза;

– с отсутствием отработанных методов и алгоритмов для оценивания эффективности средств защиты информационных ресурсов ИОС вуза.

В условиях роста количества и сложности деструктивных воздействий со стороны злоумышленников (хакеров) на различные компьютеризированные системы (например, ИОС вуза) одной из важнейших задач, стоящих перед службами эксплуатации, является задача обеспечения их КБ. Это требует соответствующего финансового инвестирования. В свою очередь принятие решений по финансированию ИБ и КБ ИОС вуза должно основываться на процедурах, позволяющих осуществлять финансирование с учетом всех факторов, присущих обеспечению надежной защиты информации.

Вопросами защиты информации и построения эффективных систем управления ИБ и КБ различных объектов информатизации, занимались многие зарубежные ученные: Д.П.Зегжда, С.В. Казмирчук, В.А.Лахно, А.Г.Корченко, В.И.Котенко, M.Atighetchi, R.H.Campbell, J. Dawkins, А.С. Марков, M.Endler. Свой вклад в исследование этих вопросов внесли и отечественные специалисты Р.Г.Бияшев, М.Н.Калимолдаев, Б.С. Ахметов, У.А.Тукеев, И.Т.Утепбергенов, В.В.Яворский, Т.С.Картбаев, Ж.К.Алимсеитова и многие другие.

Большинство исследований в области финансирования СТЗИ, в том, числе ИОС вуза, акцентированы лишь на экономической постановке задачи поиска оптимальных стратегий вложения финансовых ресурсов в средства КБ и СТЗИ. Эти работы, как правило, не учитывают тенденции, касающиеся внедрения

самых передовых информационных технологий в процедуры контроля и принятия решений для подобных проектов, а также возрастающие расходы компьютерных злоумышленников, пытающихся преодолеть контуры ИБ и КБ ради достижения своих целей.

Поэтому необходимы новые исследования в направлении развития методов и моделей для компьютерных интеллектуализированных систем поддержки принятия решений (СППР), которые позволят найти оптимальные стратегии по распределению ограниченных финансовых ресурсов учебных заведений на создание и поддержание кибербезопасной ИОС вуза.

Как показывают исследования многих ученных, посвятивших свои работы проблемам ИБ и КБ, существует явное **противоречие** между принципиальной возможностью разработки кибербезопасного объекта информатизации, в частности ИОС вуза, на базе использования современных информационных технологий (ИТ) и недостаточной эффективностью существующих систем защиты, которые не обеспечивают заданный уровень КБ в следствие недофинансирования или нерациональной финансовой стратегии стороны защиты.

Для решения, указанного выше противоречия, в диссертации поставлена новая научная задача, которая заключается в разработке моделей, методов и ИТ построения многомодульной СППР в задачах поиска стратегий защитника ИОС вуза, что позволит уменьшить расхождения данных прогнозирования и реальной отдачи от инвестирования в СТЗИ и КБ ИОС вуза, а также получить оптимальные стратегии финансирования стороной защиты СТЗИ и КБ для конкретной ИОС вуза. Поэтому, тематика диссертационной работы, которая направлена на научное обоснование моделей, методов и ИТ построения СППР в задачах поиска стратегий защиты ИОС вуза является актуальной и представляет научный и практический интерес.

Цель исследования: развитие моделей и методов защиты информационно-образовательной среды вузов на основе комплексного поиска, в том числе с применением систем поддержки принятия решений, оптимальных финансовых стратегий стороной защиты и выработки соответствующих контрмер в условиях постоянного увеличения количества дестабилизирующих воздействий на конфиденциальность, целостность и доступность информации в ИОС вуза.

Объект исследования: процессы распределения ресурсов, выделяемых на средства защиты информации и кибербезопасность ИОС вуза.

Предметом исследования являются методы и модели интегрированной защиты информационной образовательной среды вуза.

Гипотеза исследования: если, необходимо выбрать оптимальную финансовую стратегию защиты информационно образовательной среды вуза, то эффективно и комплексно решить данную задачу можно путём применения интеллектуальных систем поддержки принятия решений. Вычислительное ядро СППР содержит методы и модели, в частности, базирующиеся на теории

билинейных многошаговых игр качества с зависимыми движениями, теории сетей Петри и др. Эти методы и модели в совокупности позволяют определять множества предпочтительности и рациональные стратегии защитника ИОС вуза.

Задачи исследования:

– выполнить обзор и анализ предшествующих исследований в сфере обеспечения защиты ИОС вуза и обосновать актуальность исследований в направлении разработки моделей для систем поддержки принятия решений (СППР) по нахождению стратегий управления инвестированием для различных соотношений параметров инвестиционного процесса в системы КБ ИОС вуза;

– разработать модель для вычислительного ядра СППР по нахождению рациональных стратегий управления инвестированием для различных соотношений параметров инвестиционного процесса в системы КБ ИОС вуза;

– разработать концептуальную модель адаптивного управления киберзащитой ИОС вуза, а также модели распределения пользовательских задач, автоматизации процедур корректировки профиля пользователя и дополнить методы контроля прав доступа в контексте сверки прав доступа в ИОС вуза;

– усовершенствовать метод многокритериальной дискретной оптимизации для решения задач оценки защищенности ИОС вуза, разработать компьютерную программу «Система поддержки принятия решений по нахождению стратегий управления инвестированием в КБ ИОС вуза» и выполнить компьютерное моделирование для разновариантных стратегий инвестирования, с целью проверки адекватности модели.

Методы исследований:

– методы системного анализа и теории сложных систем с применением аппарата сетей Петри - для описания концептуальной модели адаптивного управления киберзащитой ИОС вуза и решения задачи адаптивного управления правами доступа пользователей;

– методы теории игр для синтеза новых моделей вычислительного ядра интеллектуализированной системы поддержки принятия решений по выбору рациональной финансовой стратегии инвестирования в СТЗИ и КБ ИОС вуза; методы многокритериальной дискретной оптимизации для решения задач оценки защищенности ИОС вуза, основанные на комбинации метода дискретной оптимизации Эджворта-Парето и лексикографического метода;

– методы компьютерного и имитационного моделирования для оценки эффективности предлагаемых в диссертации решений.

Научная новизна исследования:

– предложены новые модели для вычислительного ядра интеллектуализированной СППР по выбору рациональной финансовой стратегии инвестирования в СТЗИ и КБ ИОС вуза. Новизна моделей состоит в

том, что они позволяют находить решения для билинейных многошаговых игр качества с зависимыми движениями и определять множества предпочтительности и рациональные стратегии защитника ИОС вуза;

– предложена модель для автоматизации процедур корректировки профиля пользователя для минимизации или нейтрализации киберугроз в ИОС вуза, в отличие от существующих модель базируется на математическом аппарате сетей Петри и учитывает переменные, которые позволяют уменьшить мощность подпространства состояний, что повышает результативность моделирования за счет сокращения затрат времени на принятие решений, связанных с регламентацией прав доступа пользователей к узлам ИОС вуза;

– уточнен и дополнен метод контроля прав доступа пользователей к узлам ИОС вуза, в отличие от существующих, дополнения предполагают корректировку правил и метрик безопасности на основе применения нотации сетей Петри для новых или перераспределенных задач;

– усовершенствован метод многокритериальной дискретной оптимизации для решения задач оценки защищенности ИОС вуза. В отличие от существующих, предложенный усовершенствованный метод основан на комбинации метода дискретной оптимизации Эджворта-Парето и лексикографического метода, что позволило разработать векторный критерий оценки решений, включающий в качестве составляющих два условия оптимальности: стоимостною оценку рассматриваемого варианта СТЗИ и оценку его технической эффективности для конкретной ИОС вуза.

Теоретическая значимость исследования заключается в том, что получили дальнейшее развитие модели и методы защиты ИОС вуза в условиях роста сложности деструктивного вмешательства в их работу со стороны компьютерных злоумышленников. Разработанные методы и модели позволяют находить решения для билинейных многошаговых игр качества с зависимыми движениями и определять множества предпочтительности и рациональные стратегии защитника ИОС вуза. А кроме того, предложенные модели позволяют корректировать профили пользователей в ИОС вуза для минимизации или нейтрализации киберугроз, который позволяет повысить результативность моделирования за счет сокращения затрат времени на принятие решений, связанных с регламентацией прав доступа пользователей к узлам ИОС вуза.

Практическая значимость исследования заключается в разработке прикладных программных продуктов (ПП) в среде VisualStudio 2017 для решения задач оценки защищенности ИОС вуза («Модуль СППР DSS - Метод Парето для выбора средств защиты информации (СЗИ))», реализующий алгоритмы оптимального выбора при проектировании СЗИ для ИОС вуза) и выбора рациональной финансовой стратегии для обеспечения кибербезопасности ИОС вуза («Выбор рациональной финансовой стратегии для обеспечения кибербезопасности ИОС вуза (DSS)»). Программные реализации

разработанных моделей в ПП «Метод Парето для выбора СЗИ» «Выбор рациональной финансовой стратегии для обеспечения кибербезопасности ИОС вуза позволяют 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.

Основные положения, выносимые на защиту:

– модели для интеллектуализированной системы поддержки принятия решений (СППР) по выбору рациональной финансовой стратегии инвестирования в системы защиты информации и кибербезопасности ИОС вуза;

– модель для автоматизации процедур корректировки профиля пользователя для минимизации или нейтрализации киберугроз в ИОС вуза;

– метод контроля прав доступа к узлам ИОС вуза;

– усовершенствованный метод многокритериальной дискретной оптимизации для решения задач оценки защищенности ИОС вуза.

Личный вклад соискателя: все основные результаты диссертационной работы, выносимые на защиту, полученные соискателем лично, среди них:

– модели для вычислительного ядра интеллектуализированной СППР по выбору рациональной финансовой стратегии инвестирования в СТЗИ и КБ ИОС вуза;

– модель для автоматизации процедур корректировки профиля пользователя для минимизации или нейтрализации киберугроз в ИОС вуза;

– метод контроля прав доступа к узлам ИОС вуза;

– усовершенствованный метод многокритериальной дискретной оптимизации для решения задач оценки защищенности ИОС вуза.

Связь темы с планами научно-исследовательских программ: диссертационная работа выполнена в международном научно-исследовательском проекте 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).

Апробация результатов диссертации: основные положения и результаты исследования обсуждены на международных научно-практических конференциях: «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), а также на научно-методических семинарах «Информатизации образования и проблемы обучения» и на заседаниях кафедры информатики и информатизации образования Казахского национального педагогического университета имени Абая.

Результаты диссертации внедрены: в учебный процесс факультета ИТ НУБИП Украины (Акт о внедрении № 16-35 от 12.03.2020); в учебный процесс факультета ИКТ университета имени Шакарима города Семей НАО (Акт о внедрении № 255 от 10.08.2020); протестировано в лаборатории ТОО «Kaspersky LAB KZ» (Акт внедрения Республика Казахстан от 10.02.2020).

Применение разработанных программных продуктов позволило сократить затраты на построение контуров кибербезопасности ИОС вуза примерно на 11–14 % по сравнению первоначальными плановыми параметрами.

Предложенные методы, модели и разработанные ПП могут быть использованы для повышения степени киберзащищенностии других ИОС вуза Казахстана.

Публикации по результатам исследования: результаты исследования нашли отражения в 21 печатных работах, из которых 3 – в журналах, входящих в базу данных Scopus, 5 – в изданиях, рекомендуемых Комитетом по обеспечению в сфере образования и науки Министерства образования и науки Республики Казахстан, 11 – в сборниках материалов международных научно-практических конференций (из них 7 – в сборниках материалов зарубежных конференций), 2 - в зарубежных научных журналах.

Структура диссертации: диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений.

ANNOTATION
of dissertation work by Kydyralina Lazat Muktarovna
"Methods and models of integrated protection of the educational information environment of the university",
submitted for the degree of Doctor of Philosophy (PhD)
on the specialty 6D060200 – Informatics

The relevance of research: A key role in the development and improvement of the efficiency of the activities of universities is played by its orientation towards the constant search and application of the latest approaches, technologies and means that appear in the world as science and technology develop. In this regard, universities cannot remain aside from the global processes of digitalization and informatization, especially relevant in recent years in connection with the selection and formation of new types of technologies and means attributed to the fourth industrial revolution. Such technologies allow technical means to interact with each other without human intervention. An additional incentive for the development of educational systems is the formation of new generations of people who are ready and able to live and learn, using digital technologies everywhere.

In connection with these and other factors, timely complex and comprehensive digitalization becomes strategic in nature, requires the search and systematization of appropriate conceptual approaches. A striking example is the concept of digitization of the Kazakh National Pedagogical University named after Abay, developed under the guidance of Professor T.O.Balykbayev and Professor E.Y. Bidaibekov. The concept is aimed at ensuring the integrity and long-term systematic development of approaches to the integration and use of digital technologies and means in order to increase efficiency of all types of activities of KazNPU named after Abay as a digital university. The content of the concept was formed taking into account the results of the analysis of the digital infrastructure of the university, on the basis of which there were determined the priority directions of digitalization of the university. There are considered theoretical and practical foundations of digitalization of educational and educational-methodical activities, scientific research and integration of the university into the world scientific community, approaches to the development of digital competence of students and teachers in the context of digitalization of the university.

The Concept pays special attention to issues of information security (IS) and cybersecurity (CS) of the digital educational environment of the university. In modern universities, there are working a large number of teachers, researchers, thousands, and sometimes tens of thousands of students are studying, who make up the intellectual and labor potential of the development of any state. In this connection, the task of providing IS and CS of universities and other educational institutions in modern conditions is of great importance.

It should be noted that there are a number of problems in the field of IS and CS management of university, among which the most significant are: poor equipment of

IEEU with means of technical protection of information resources (IPTM); the existing moral and physical deterioration of the equipment that provides solutions to the tasks of providing CS (switches, routers, firewalls, etc.); the absence of specially trained specialists in the staffing tables of the IT departments of informatization of universities, who are responsible specifically for the issues of IS and CS of the university, who could competently and optimally distribute the targeted funding that is allocated to provide the CS of IEEU.

The existing approaches to the issues of CS of IEEU are mainly based on solutions that are typical mainly for commercial enterprises or so-called secure facilities. However, educational institutions and universities, in particular, have their own specifics. Designers of CS of IEEU systems note the following difficulties in the process of creating IS control systems:

– the absence of special techniques and methods for assessing the current state of IS and CS of the university;

– uncertainty and specificity of destabilizing factors that can affect the protected resources of IEEU;

– the absence of proven methods and algorithms for assessing the effectiveness of means of protecting information resources of IEEU.

In the context of the growing number and complexity of destructive influences on the part of intruders (hackers) on various computerized systems (for example, IEEU), one of the most important tasks facing the operation services is the task of providing their CS. This requires appropriate financial investment. In turn, decision-making on the financing of IS and CS of IEEU should be based on procedures that allow financing taking into account all the factors inherent to ensuring reliable information protection.

The issues of information security and the creation of effective information security and cybersecurity systems for various objects of informatization were dealt with by many domestic and foreign scientists, in particular: D.P. Zegzhda, S.V. Kazmirchuk, V.A. Lakhno, A.G. Korchenko, V.I. Kotenko, M. Atighetchi, R.H. Campbell, J. Dawkins, A.S. Markov, M.Endler. Domestic experts also contributed to the study of these issues R. G. Biyashev, M. N. Kalimoldayev, B. S. Akhmetov, W. A. Tukeev, I. T. Utepbergenov, V., Jaworski, T. S. Kartbayev, Zh. K. Alimseitova and many others.

Most of the studies in the field of financing IPTM, including IEEU, are focused only on the economic formulation of the problem of finding optimal strategies for investing financial resources in the funds of CS and IPTM. These works, as a rule, do not take into account the trends regarding the implementation of the most advanced information technologies in the control and decision-making procedures for such projects, as well as the increasing costs of computer attackers trying to overcome the contours of IS and CS in order to achieve their goals.

Therefore, new research is needed in the direction of developing methods and models for computer intelligent decision support systems (DSS), which will make it possible to find optimal strategies for the allocation of limited financial resources of educational institutions for the creation and maintenance of cybersecure IEEU.

As the studies of many scientists who have devoted their work to the problems of IS and CS show, there is a clear **contradiction** between the fundamental possibility of developing a cybersecure object of informatization, in particular IEEU, based on the use of modern information technologies (IT) and the insufficient effectiveness of existing protection systems that do not provide a given level of CS due to underfunding or irrational financial strategy of the protection.

In order to solve the above contradiction, the dissertation posed a new scientific task, which consists in the development of models, methods and IT for creating a multi-module DSS in the problems of finding strategies for the protection of IEEU, which will reduce the discrepancy between the prediction data and the real return on investment in IPTM and CS of IEEU, as well as to obtain the optimal financing strategies for the protection of IPTM and CS for a specific IEEU. Therefore, the topic of the dissertation work, which is aimed at the scientific substantiation of models, methods and IT for creating a DSS in the tasks of finding strategies for protection of IEEU is relevant and is of scientific and practical interest.

Purpose of the research: the purpose of the dissertation work is to develop models and methods for protecting the information and educational environment of universities on the basis of an integrated search, including the use of decision support systems, optimal financial strategies by the protection side and the development of appropriate countermeasures in conditions of a constant increase in the number of destabilizing impacts on confidentiality, integrity and availability of information in IEEU.

The object of the research: is the processes of resource allocation for information security and cybersecurity of IEEU.

The subject of the research is methods and models of integrated protection of the educational information environment of the university.

Research hypothesis: if it is necessary to choose the optimal financial component of the strategy for protecting the information and educational environment of the university, then this problem can be effectively and comprehensively solved by using intelligent decision support systems. The computing core of which contains methods and models, in particular, based on the theory of bilinear multi-stage quality games with dependent movements, the theory of Petri nets, etc. These methods and models which together allows to determine the sets of preferences and rational strategies of the IEEU protector. these methods and models

Research objectives:

– to review and analyze previous research in the field of ensuring the protection of IEEU and substantiate the relevance of research in the direction of developing models for decision support systems (DSS) in order to find investment management

strategies for various ratios of the parameters of the investment process in CS systems of IEEU;

– to develop a model for the computational core of the DSS for finding rational investment management strategies for various ratios of the parameters of the investment process in the CS IEE system of the university;

– to develop a conceptual model of adaptive management of the CS IEE of the university, as well as a model for distributing user tasks, automating procedures for adjusting the user profile, and to complement methods for access rights control in the context of access rights verification in the IEE of the university;

– to improve the method of multicriteria discrete optimization for solving the tasks of assessing the security of the IEE of the university, to develop a computer program "Decision support system for finding investment management strategies in the CS IEE of the university" and to perform computer modeling for different investment strategies in order to check the adequacy of the model.

Research methods:

– methods of system analysis and the theory of complex systems using the apparatus of Petri nets - to describe the conceptual model of adaptive control of CS of IEEU and to solve the problem of adaptive control of user access rights;

– methods of game theory for the synthesis of new models of the computing core of an intellectualized decision support system for choosing a rational financial strategy for investing in IPTM and CS of IEEU;

– methods of multicriteria discrete optimization for solving problems of assessing the security of IEEU, based on a combination of the Edgeworth-Pareto discrete optimization method and the lexicographic method;

– methods of computer and simulation modeling for assessing the effectiveness of the solutions proposed in the dissertation.

Scientific novelty of the research:

– there were proposed new models for the computing core of an intellectualized DSS for choosing a rational financial strategy for investing in IPTM and CS of IEEU. The novelty of the models lies in the fact that they allow to find solutions for bilinear multi-step quality games with dependent movements and to determine the sets of preferences and rational strategies of the IEEU defender;

– there was proposed a model for automating the procedures for adjusting the user profile in order to minimize or neutralize cyber threats in IEEU, in comparison to the existing model, it is based on the mathematical apparatus of Petri nets and takes into account variables that allow reducing the power of the state subspace, which increases the effectiveness of modeling due to reducing the time spent on decision making related to the regulation of user access rights to IEEU nodes;

– there was clarified and supplemented the method for controlling user access rights to IEEU nodes, in comparison to the existing ones, the additions imply the

adjustment of security rules and metrics based on the application of the Petri nets notation for new or redistributed tasks;

– there was improved the method of multicriteria discrete optimization for solving problems of assessing the security of IEEU. In comparison to the existing ones, the proposed improved method is based on a combination of the Edgeworth-Pareto discrete optimization method and the lexicographic method, which made it possible to develop a vector criterion for assessing solutions, including two optimality conditions as components: the cost estimate of the considered IPTM variant and the assessment of its technical efficiency for a specific IEEU.

The theoretical significance of the research lies in the fact that the models and methods of protecting IEEU have been further developed in conditions of increasing complexity of destructive interference in their work by computer intruders. The developed methods and models make it possible to find solutions for bilinear multi-step quality games with dependent movements and to determine the sets of preferences and rational strategies of the IEEU protector. In addition, the proposed models allow to adjust user profiles in IEEU in order to minimize or neutralize cyber threats, that allows to increase the effectiveness of modeling by reducing the time spent on decision making related to the regulation of user access rights to IEEU nodes.

The practical significance of the results obtained for universities lies in the development of applied software products (SP) in the VisualStudio 2017 environment for solving problems of assessing the security of IEEU ("DSS DSS Module - Pareto Method for the Selection of Information Protection Means (IPM)"), which implements optimal choice algorithms for the design of IPM of IEEU) and the choice of a rational financial strategy for ensuring the cybersecurity of IEEU ("Choosing a rational financial strategy for ensuring cybersecurity of IEEU (DSS)"). Software implementations of the developed models in the "Pareto method for choosing IPM", "Choosing a rational financial strategy to ensure the cybersecurity of IEEU" allows to select the optimal financial strategy component of the protection side for any ratio of parameters describing the financing process, no matter how financially the second party tries to break the perimeters of IEEU protection.

The main provisions for the defense:

– models for an decision support system (DSS) for choosing a rational financial strategy for investing in information security and cybersecurity systems of IEEU;

– a model for automating procedures for adjusting the user profile in order to minimize or neutralize cyberthreats in IEEU;

– method of access rights control to IEEU nodes;

– an improved method of multicriteria discrete optimization for solving problems of assessing the security of IEEU.

Personal contribution of the applicant: all the main results of the dissertation work submitted for defense, received by the applicant personally, among them:

– *models* for the computing core of an intellectualized DSS for choosing a rational financial strategy for investing in IPTM and CS of IEEU;

– *a model* for automating the procedures for adjusting the user profile in order to minimize or neutralize cyber threats in IEEU;

– method of controlling access rights nodes of IEEU;

– an improved method of multicriteria discrete optimization for solving problems of security assessment of IEEU.

Connection of the topic with the plans of research programs: the dissertation work was carried out in the international research project of KazNPU named after Abay with the Research Institute Higher School of Economics (Russia, Moscow) on the topic "Monitoring the penetration of digital tools into the educational process of the university" (research agreement No. 19/04 dated 19.04.2019).

Approbation of the dissertation results: the main provisions and results of the research were discussed at international scientific and practical conferences: «Part of the Advances in Intelligent Systems and Computing book series» (Warsaw, 2018), «Current issues of cybersecurity and information security» (Kiev, 2018), «Problems of technology and telecommunications technology» (Uralsk, 2018), «Status and improvement of security of information and telecommunication systems» (Ukraine, 2018), «Problems of Informatics in Education, Management, Economics and Technology» (Penza, 2018), «New Information Technologies and Systems» (Penza, 2018), «The goals of sustainable development of the third millennium: challenges for universities of life sciences» (Kiev, 2018), «International Journal of Civil Engineering and Technology» (India, -2019), «Topical issues of economic and social development in the context of digitalization» (Semey, 2019), «University - oh-pikirler aimagy» (Aktau, 2019), «Mathematicalyk modeldeu men akparatttyk tekhnologar bilimde zhane gylymda» (Almaty, 2020), as well as at scientific and methodological seminars "Informatization of education and learning problems" and at meetings of the Department of Informatics and Informatization of Education of the Kazakh National Pedagogical University named after Abai.

The results of the dissertation are implemented:work were introduced in the educational process of the IT Faculty of the NUBNM of Ukraine (Act of Implementation No. 16-35 dated 12.03.2020); of the ICT Faculty of the Shakarim University of Semey (Act of Implementation No. 255 dated 10.08.2020); tested the Republic of Kazakhstan the lab LLP «Kaspersky LAB KZ» (Act of Implementation dated 10.02.2020).

The use of the developed software products made it possible to reduce the costs on creating the IEEU cybersecurity contours by about 11-14% compared to the initial planned parameters.

The proposed methods, models and developed software programs can be used to increase the degree of cybersecurity of other IEEUs in Kazakhstan.

Research publications: the results of the study were reflected in 21 printed works, 3 of which - in journals included in the Scopus database, 5 - in publications recommended by the Committee for Control in Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan, 11 - in collections of materials of international scientific-practical conferences (7-of them are in the collections of materials of foreign conferences), 2 - of foreign scientific journals.

The structure of the dissertation work: the dissertation consists of an introduction, four chapters, conclusion, references and appendices.