Адранова Асельхан Багдатовнаның
6D060200 – «Информатика» мамандығы бойынша философия докторы (PhD) дәрежесін алу үшін ұсынған «Қашықтықтан оқытудың ақпараттық қауіпсіздігін қамтамасыз етудің модельдері, әдістері және алгоритмдері» тақырыбындағы диссертациясына

АҢДАТПА

Зерттеудің өзектілігі: ЖОО-да жаңа цифрлық технологияларды қолданудың ұлғайып келе жатқан ауқымы, ақпараттық платформаларды және жүйелерді, атап айтқанда қашықтықтан оқыту мәселелерінде пайдалану, оқу процесіне инновациялық аппараттық-бағдарламалық құралдарды іс жүзінде жүзеге асыру, оқу орындарының ақпараттық-білім беру ортасын олардың жұмысына араласудың ұлғайып келе жатқан қиындықтары мен саны аясында осал етеді. Бұл ретте, жоғары оқу орындарының қашықтықтан оқыту жүйелерінде сақталатын және айналыстағы қорғалатын мәліметтерге мыналарды жатқызуға болады: студенттердің, оқытушылардың, ғылыми қызметкерлердің дербес деректері; оқу орнының интелектуалдық меншігін білдіретін цифрланған ақпарат; оқу процесін қамтамасыз ететін ақпараттық массивтер (мысалы, мультимедиалық контент, мәліметтер базасы, білім беру және басқа да жеке жобалау бағдарламалары және бөгде бағдарламалық өнімдер) және тағы басқалар. ЖОО-ның қашықтықтан оқыту жүйесінде аталған ақпараттық ресурстар сыртқы (ішкі) компьютерлік қаскүнемдер тарапынан ұрлау немесе бұрмалау нысаны ретінде, студенттер мен қызметкерлер тарапынан бұзақылық ниеттен болуы мүмкін.

Көптеген постиндустриялық елдерде қалыптасқан ЖОО-ның қашықтықтан оқыту жүйесіне (ҚОЖ) қолжетімділікті жаһандандыру үрдісі неғұрлым сенімді қорғау проблематикасын зерделеуге және жалпы ЖОО-ның киберқауіпсіздігінің перспективалық стратегияларын әзірлеуге байланысты маңызды мәселелерді қарастырады.

Бұл ретте бірнеше рет резервтеуге, кіріктірілген вирусқа қарсы бақылау жүйелерін және сенімділіктің жоғары деңгейі бар элементтерді енгізуге негізделген ҚОЖ-н қорғау контурын құрудың дәстүрлі әдістері жобаланатын және қолданыстағы ҚОЖ-нің техникалық-экономикалық сипаттамаларын нашарлатады. Бұдан басқа, мұндай тәсіл ЖОО-ның ҚОЖ-дегі контентті бұрмалауға немесе ауыстыруға, сондай-ақ олардың жалпы жұмысының сенімділігін қамтамасыз етуге байланысты қатерлі жағдайлардың туындау ықтималдығының қажетті азаюына әкеп соқтырмайды.

Қазіргі заманғы ЖОО-да ақпараттық-коммуникациялық технологиялар, атап айтқанда ҚОЖ оқу процесінің негізгі элементтерінің бірі. Қазіргі заманғы оқу орындары саяси және әлеуметтік саланың элементтері ретінде ақпараттық ресурстар және ақпараттық технологиялармен тікелей байланысты. Қазіргі заманғы ҚОЖ және оның ақпараттық желісінің негізгі компоненттері компьютерлік технологиялар, бұлтты технологиялар, мобильді технологиялар, ақпараттық қауіпсіздік технологиялары, деректерді

өңдеудің қазіргі заманғы орталықтарының технологиялары және т.б. Олар өзара тығыз байланысты және өз кезегінде ЖОО-ның ҚОЖ-нің бағдарламалық-аппараттық кешеніне әсер етеді. Сондықтан, бір жағынан, білім алушылардың ҚОЖ-нің АТ-ресурстарына, АТ-инфрақұрылымына барынша жылдам қол жеткізуін қамтамасыз ететін түрлі жаңа инновациялық шешімдерді енгізу қажеттілігі туындайды. Ал екінші жағынан, нақты уақытта ҚОЖ жұмысының функционалды тұрақтылығын және киберқауіпсіздігін қамтамасыз ету.

Күрделі бөлінген есептеу желілерінің ақпаратты қорғау жүйелерінің тиімділігін жоғарылату саласындағы зерттеулердің көпшілігі, оларға қашықтықтан оқыту жүйелерін, сондай-ақ киберқауіпсіздік және ақпаратты қорғау жүйелеріне қаржы ресурстарын салудың оңтайлы стратегияларын іздеу мәселесін экономикалық тұрғыдан қоюға ғана назар аударылған білім беру процесіне белсенді енгізілетін виртуалдық бұлттық технологияларды да жатқызуға болады. Бұл жұмыстар, әдетте, осындай жобалар үшін шешімдер қабылдауға және бақылау процедураларына ең озық ақпараттық технологияларды енгізуге қатысты үрдістерді ескермейді. ҚОЖ-дегі киберқатерлерге қарсы тұру үшін қарсы шараларды таңдауға жұмсалатын қаржы ресурстарын бөлу бойынша көптеген модельдердің кемшілігі - киберқауіпсіздік және ақпаратты қорғау жүйесіне қаржылық инвестициялар стратегияларын қалыптастыру бойынша нақты ұсынымдардың болмауы.

Сондықтан шешімдерді қолдаудың компьютерлік жүйелері үшін әдістер мен модельдерді дамыту бағытында жаңа зерттеулер жүргізу қажет, олар ЖОО-ның шектеулі қаржы ресурстарын бөлу бойынша, жалпы ҚОЖ-нің функционалды тұрақтылығы мен киберқауіпсіздігін құру және қолдау үшін оңтайлы стратегияларын табуға мүмкіндік береді.

Ақпаратты қорғау және ақпараттандырудың әртүрлі нысандарының ақпараттық қауіпсіздігін басқарудың тиімді жүйелерін құру мәселелерімен көптеген отандық және шетелдік ғалымдар айналысты, атап айтқанда: Б.С. Ахметов, Р.Г.Бияшев, А.В. Барабанов, Д.П. Зегжда, М.Н.Калимолдаев, С.В.Казмирчук, А.Г. Корченко, Т.С.Картбаев, В.А. Лахно, В.В. Малюков, А.С. Марков, У.А. Тукеев, В.Л.Цирлов, M. Atighetchi, R.H. Campbell, J. Dawkins және т.б. Олардың зерттеулері көрсеткендей, ЖОО-ның ҚОЖ-нің рұқсатсыз қолжетімділігі мен шабуылдарға функционалды тұрақтылығын құрудың мүмкіндігімен және олардың функционалды тұрақтылығы мен киберқауіпсіздігінің қажетті деңгейін қамтамасыз ете алмайтын ЖОО-ның қашықтықтан оқыту жүйелерін қорғаудың қолданыстағы жүйелерінің тиімділігінің жеткіліксіздігі арасында айқын қарама-қайшылық бар.

Жоғарыда көрсетілген қайшылықты шешу үшін диссертацияда ғылыми мақсат қойылған, ол қолданыстағы және перспективті ақпараттық желілер негізінде ЖОО-ның ҚОЖ-н қорғалған және функционалды тұрақтылығын құрудың модельдерін, әдістері мен ақпараттық технологияларын құрудан тұрады. Сондықтан осы мәселені шешуге бағытталған диссертациялық жұмыстың тақырыбы өзекті және ғылыми және практикалық қызығушылық танытады.

Зерттеудің мақсаты: ҚОЖ үшін киберқауіптерді анықтау арқылы деструктивті әсерлердің саны үнемі өсуі жағдайында ҚОЖ-н қорғау үшін пайдаланатын модельдерді, әдістерді және ақпараттық технологияларды дамыту және сәйкес қарсы шараларды таңдау.

Зерттеудің нысаны: ҚОЖ-нің функционалды тұрақтылығын қамтамасыз ету және киберқатерді анықтау процестері.

Зерттеудің пәні: ЖОО-ның ҚОЖ-нің ақпараттық қауіпсіздігін қамтамасыз ету әдістері мен модельдері.

Зерттеудің ғылыми болжамы: егер, ЖОО ҚОЖ-нің ақпараттарды қорғау және киберқауіпсіздік дәрежесін арттыру талап етілсе, онда бұл міндетті шешу ҚОЖ-і үшін ағымдағы және жаңа киберқатерлерді анықтау әдістері мен модельдерін кешенді қолдану және осы қатерлерге сәйкес келетін қарсы шараларды таңдау арқылы жүзеге асырылады.

Зерттеудің міндеттері:

− қазіргі заманғы жоғары оқу орындарының цифрлық білім беру ортасын (ЖООЦББО) және оның компоненттері-қашықтықтан оқыту жүйесінің (ҚОЖ) киберқорғаудың базалық тәсілін талдау, сондай-ақ ҚОЖ-нің виртуалды бұлтты ресурстарының функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету бойынша мәселелерді талдау;

− ҚОЖ-нің ақпаратты қорғау жүйесін сипаттау үшін модельдерді құру;

− ҚОЖ-де киберқатерді анықтау әдісін жетілдіру;

− ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін виртуалды бұлтты ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін математикалық модельдерді жетілдіру, сондай-ақ бағдарламалық-конфигурацияланатын желілерді қолдану негізінде виртуалды бұлтты ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету әдістемесін құру;

− ҚОЖ-нің киберқауіпсіздігін және ақпаратты қорғау жүйесін құрудың оңтайлы нұсқасын таңдау әдістемесін жетілдіру.

Зерттеудің әдістері: Зерттеу барысында пәндік аймақтың ерекшеліктерін және тұжырымдалған мәселелерді ескере отырып, келесі әдістер қолданылды: жүйелік талдау және күрделі жүйелер теориясы (бұл ЖОО-ның ҚОЖ-нің иерархиялық ақпараттық желісін кездейсоқ жұмыс процесінің күйі мен ауысу графигін сипаттау үшін); ЖОО–ның ҚОЖ-нің ақпараттық желісінің функционалды тұрақтылығы мен киберқауіпсіздігінің теориялық негіздері (ҚОЖ-нің сенімділігін модельдеу үшін); сараптамалық бағалау әдістері, комбинаторлық теория және аналитикалық модельдеу (виртуалды бұлтты ресурстардың киберқауіпсіздігін және функционалды тұрақтылығын қамтамасыз етудің математикалық моделін жетілдіру үшін); жаппай қызмет көрсету теориясы мен ойындар теориясының жалпы ережелері (ҚОЖ-нің киберқауіпсіздігін және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдаудың әдістемелерін жетілдіру үшін).

Зерттеудің ғылыми жаңалығы:

− марковтық тізбектер негізінде ҚОЖ-нің киберқатерін сипаттау үшін модель алынды, ол ЖООЦББО және ҚОЖ-не шабуыл қатерінің нақты

марковтық модельдерін құруға мүмкіндік береді және ҚОЖ-нің киберқауіпсіздігін инвестициялаудың рационалды стратегиясын таңдау алгоритмдері мен модельдерімен бірге ҚОЖ қорғалған және функционалды тұрақтылығын құру әдіснамасын жетілдіруге мүмкіндік береді;

− ҚОЖ-де киберқатерді анықтау әдісі жетілдірілді, ол қолданыстағы әдістерден айырмашылығы үлестірілген желіні өздігінен оқуға арналған рекурсивті алгоритмдерді және киберқатер түріне байланысты қарсы шараларды (стратегияларды, атап айтқанда ҚОЖ-н қорғау жағынан қаржылық немесе техникалық) таңдау;

− ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін ВБР-дың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін математикалық модель жетілдірілді. Бұл модельдің қолданыстағы модельдерден айырмашылығы бағдарламалық-конфигурацияланатын желілер үшін кешенді көрсеткіш негізінде мүмкін қарсы шараларды таңдау және виртуалды бұлтты ресурстардың жағдайын ескереді, сондай-ақ виртуалды бұлтты ортаға шабуыл графтарды қолдану процедурасы есебінен жүйенің барлық белгілі осалдықтары туралы ақпарат алуға мүмкіндік береді, сондай-ақ нақты уақыт режимінде ВБР-дың функционалды тұрақтылығы мен киберқауіпсіздігі жағдайын көрсетеді;

− ҚОЖ-нің киберқауіпсіздік және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдау әдістемесі дамытылды, әдістеменің қолданыстағы әдістемелерден айырмашылығы, ақпараттық желіде және ҚОЖ-де киберқатерді анықтаудың жетілдірілген әдісімен, жаппай қызмет көрсету жүйесі (ЖҚКЖ) ретінде ҚОЖ-нің ақпараттық қауіпсіздігін басқару жүйесінің моделі, оқу орнының шектеулі бюджеті жағдайында ақпаратты қорғау құралдарын тиімді және ұтымды іздеу үшін антагонистік ойын моделімен толықтырылған.

Зерттеудің теориялық маңыздылығы: Компьютерлік қаскүнемдер тарапынан олардың жұмысына деструктивті араласу күрделілігінің өсуі жағдайында ҚОЖ-н қорғаудың модельдері мен әдістері одан әрі дамытылды. Бұл ретте алғаш рет Марков тізбектеріне негізделген ҚОЖ-нің киберқатерлерін сипаттауға арналған модель алынды, ол ҚОЖ-не шабуыл жасау қатерінің нақты марковтық модельдерін құруға мүмкіндік береді. Сондай-ақ, ҚОЖ-дегі киберқатерлерді анықтау әдісі жетілдірілді, ол қолданыстағы әдістерден айырмашылығы үлестірілген желіні өздігінен оқуға арналған рекурсивті алгоритмдерден тұрады және ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін виртуалдық бұлттық ортаның (ВБО) функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз етуге арналған модель жетілдірілді, ол қолданыстағы модельдерден айырмашылығы ЖОО-ның бұлтты ортасының жай-күйін ескереді және бағдарламалық-конфигурацияланатын желілер үшін кешенді көрсеткіш негізінде ықтимал қарсы шараларды таңдауды жүзеге асыруға мүмкіндік береді.

Зерттеудің практикалық маңыздылығы: Rad Studio 10.3 ортасында қолданбалы бағдарламалық өнімдерді (БӨ) құру. Әзірленген БӨ ҚОЖ-нің

ақпараттық қауіпсіздігін басқару жүйесін жобалау процесінің жоғары тиімділігін қамтамасыз етеді және ҚОЖ үшін қолайлы тәуекел деңгейін интерпретациялау нәтижелерінің дұрыстығын арттырады. Әзірленген бағдарламалық өнімдер негізінде жүргізілген есептеу эксперименттері диссертациялық жұмыстың негізгі теориялық маңыздылығының дұрыстығын растады. Ұсынылған шешімдер жалпы алғанда ҚОЖ-н және ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздік көрсеткішін белгілі шешімдермен салыстырғанда 12-17%-ға арттыруға мүмкіндік беретіні эксперименталды көрсетілді.

Ұсынылған әдістер, модельдер және әзірленген бағдарламалық өнімдер ЖОО-ның ҚОЖ-нің киберқорғалу дәрежесін арттыру үшін пайдаланылуы мүмкін.

Қорғауға ұсынылатын негізгі қағидалар:

− марковтық тізбектер негізінде қашықтықтан оқыту жүйесінің киберқатерін сипаттау үшін модель;

− киберқатерлер түріне байланысты қарсы шараларды таңдау және үлестірілген желіні өздігінен оқуға арналған рекурсивті алгоритмдерді қамтитын қашықтықтан оқыту жүйелерінде киберқатерлерді анықтау әдісі;

− қашықтықтан оқыту жүйесінің бағдарламалық-конфигурацияланатын желілері үшін виртуалды бұлтты ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету моделі;

− қашықтықтан оқыту жүйелерінің киберқауіпсіздігін және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдау әдістемесі.

Ізденушінің жеке үлесі. Қорғауға шығарылатын диссертацияның барлық негізгі нәтижелері ізденушімен жасалған, олардың ішінде: жоғары оқу орындарының қашықтықтан оқыту жүйесінің бағдарламалық-конфигурацияланатын желілері үшін виртуалды бұлтты ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету алгоритмдері мен модельдері; жаппай қызмет көрсету жүйесі ретінде қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздікті басқару жүйесінің компьютерлік моделі.

Зерттеудің нәтижелерін сынақтан өткізу: Абай атындағы Қазақ ұлттық педагогикалық университетінің «Информатика және білімді ақпараттандыру» кафедрасының «Білімді ақпараттандыру және оқыту мәселелері» ғылыми-әдістемелік семинарында, Биоресурстарды және табиғатты пайдалану ұлттық университетінің (Украина) «Ақпараттық технологиялар» факультеттерінде, сонымен бірге халықаралық ғылыми-әдістемелік конференцияларда: «Білім берудегі ғылым мен практикадағы заманауи ақпараттық-коммуникациялық технологиялар» атты республикалық ғылыми-практикалық конференция, (Алматы, 2018); «Өнеркәсіптегі цифрлық технологиялар» атты республикалық ғылыми-практикалық конференция, (Ақтау, 2019); «Инновациялық технологиялар – ҚР-сы экономикасының кен және мұнай-газ секторларындағы іргелі және қолданбалы мәселелерді табысты шешудің кілті» атты халықаралық Сәтбаев оқулары, (Алматы, 2019); «Математикалық модельдеу мен ақпараттық технологиялар білімде және

ғылымда» атты IX Халықаралық ғылыми-әдістемелік конференция (Алматы, 2020); «Безпека ресурсів інформаційних систем» атты I халықаралық ғылыми-практикалық конференциясында (Чернигов, 2020) баяндалды.

Сонымен қатар, Абай атындағы Қазақ ұлттық педагогикалық университетінің «біліктілікті арттыру және қашықтықтан білім беру» орталығына, Алматы энергетика және байланыс университетінің «Басқару жүйелері және ақпараттық технологиялар» институтында, Биоресурстарды және табиғатты пайдалану ұлттық университетінің (Украина) «Ақпараттық технологиялар» факультетінде (акт №16-34, 12.03.2020ж.) оқу процесіне ендірілді.

Жарияланымдар: Диссертация тақырыбы бойынша 14 жарияланым бар, оның 6 - ҚР БҒМ Білім және ғылым саласында сапаны қамтамасыз ету комитеті ұсынған басылымдарда, 3 мақала Scopus мәліметтер қорына кіретін басылымда, 1 мақала жақын шетелдік ғылыми конференцияда, 4 мақала халықаралық ғылыми-тәжірибелік конференция жинақтарында жарияланған.

Диссертацияның құрылымы: Диссертациялық жұмыс, кіріспеден, үш тараудан, қорытындыдан, пайдаланылған әдебиеттер тізімінен және қосымшалардан тұрады.

АННОТАЦИЯ
диссертационной работы Адрановой Асельхан Багдатовны
«Модели, методы и алгоритмы обеспечения информационной безопасности дистанционного обучения» представленной на соискание степени доктора философии (PhD) по специальности
6D060200 – «Информатика»

Актуальность исследования: Увеличивающиеся масштабы применения новых цифровых технологий в университетах, использование информационных платформ и систем, в частности облачных, в задачах дистанционного образования, имплементация в учебный процесс инновационных аппаратно-программных средств, делают информационно-образовательную среду учебных заведений уязвимой на фоне возрастающей сложности и количества деструктивных попыток вмешательства в их работу. При этом полагаем, что к защищаемым сведениям, которые хранятся и циркулируют в системах дистанционного образования (СДО) вузов можно отнести: персональные данные учащихся, преподавателей, научных сотрудников; оцифрованную информацию, представляющую интеллектуальную собственность учебного заведения; информационные массивы, которые, обеспечивают учебный процесс, (например, мультимедийный контент, базы данных, обучающие и иные программы собственной разработки и сторонние программные продукты) и многое другое. Перечисленные информационные ресурсы в СДО вуза могут выступить как объект хищения или искажения со стороны внешних (внутренних) компьютерных злоумышленников или из хулиганских побуждений со стороны учащихся или сотрудников.

Сформированный во многих постиндустриальных странах тренд на глобализацию доступа к СДО вузов делает релевантными задачи, связанные с изучением проблематики их более надежной защиты и разработкой перспективных стратегий кибербезопасности (КБ) вузов в целом.

При этом традиционные методы к построению контуров защиты СДО, основанные на многократном резервировании, введении систем встроенного антивирусного контроля и элементов с повышенным уровнем надежности ухудшают технико-экономические характеристики проектируемых и существующих систем дистанционного обучения. Кроме того, часто подобный подход не приводит к необходимому уменьшению вероятности возникновения опасных ситуаций, связанных с искажением или подменой контента в СДО вузов, а также с обеспечением надежности их работы в целом.

Информационно-коммуникационные технологии в вузах, в частности СДО, являются одними из ключевых элементов учебного процесса. Заметим, что современные учебные заведения, как элементы политической и социальной сферы, напрямую связаны с информационными ресурсами и информационными технологиями. Основными компонентами современной СДО и ее информационной сети (ИнС) являются компьютерные технологии,

облачные технологии, мобильные технологии, технологии информационной безопасности, технологии современных центров обработки данных и др. Они тесно взаимосвязаны между собой и, в свою очередь, влияют на программно-аппаратный комплекс СДО вуза поэтому возникает необходимость внедрять новые разнообразные инновационные решения, которые обеспечат достаточно быстрый доступ учащихся к ИТ-инфраструктуре, ИТ-ресурсам СДО с одной стороны, а с другой стороны, обеспечат функциональную устойчивость работы(ФУ) СДО и ее КБ в реальном времени.

Большинство исследований в области повышения эффективности систем защиты информации (СЗИ) сложных распределенных вычислительных сетей, к которым можно безусловно отнести и СДО, а также виртуальных облачных систем (ВОС), активно внедряемых в образовательный процесс, акцентированы лишь на экономической постановке задачи поиска оптимальных стратегий вложения финансовых ресурсов в средства КБ и СЗИ. Эти работы, как правило, не учитывают тенденции, касающиеся внедрения самых передовых информационных технологий в процедуры контроля и принятия решений для подобных проектов. Недостатком многих моделей по распределению финансовых ресурсов, затрачиваемых на выбор контрмер для противостояния киберугрозам в СДО, является отсутствие конкретных рекомендаций по формированию стратегий финансовых инвестиций в СЗИ и КБ.

Поэтому необходимы новые исследования в направлении развития методов и моделей для компьютерных систем поддержки решений, которые позволят найти оптимальные стратегии по распределению ограниченных финансовых ресурсов университетов на создание и поддержание функционально устойчивых и кибербезопасных СДО в целом.

Вопросами защиты информации и построения эффективных систем управления информационной безопасности различных объектов информатизации занимались многие отечественные и зарубежные ученые, в частности: Б.С. Ахметов, Р.Г.Бияшев, А.В. Барабанов, Д.П. Зегжда, М.Н.Калимолдаев, С.В.Казмирчук, А.Г. Корченко, Т.С.Картбаев, В.А. Лахно, В.В. Малюков, А.С. Марков, У.А. Тукеев, В.Л.Цирлов, M. Atighetchi, R.H. Campbell, J. Dawkins. Как показывают их исследования, существует явное противоречие между принципиальной возможностью разработки функционально устойчивых к атакам и несанкционированному доступу к СДО вузов и недостаточной эффективностью существующих систем защиты СДО вузов, которые не обеспечивают заданный уровень их кибербезопасности и функциональной устойчивости.

Для разрешения, указанного выше противоречия в диссертации поставлена новая научная задача, которая заключается в разработке моделей, методов и информационных технологий построения функционально устойчивой и защищённой СДО вуза на базе имеющихся и перспективных информационных сетей. Поэтому тематика диссертационной работы, которая направлена на решение этой задачи, является актуальной и представляет научный и практический интерес.

Цель исследования: Развитие моделей, методов и информационных технологий, используемых для защиты СДО в условиях постоянного увеличения количества дестабилизирующих воздействий, путем выявления киберугроз для СДО и выбора соответствующих контрмер.

Объект исследования: Процессы выявления киберугроз и обеспечение функциональной устойчивости СДО.

Предмет исследования: Модели и методы обеспечения информационной безопасности СДО вузов.

Гипотеза исследования: если, требуется повысить степень защиты информации и кибербезопасности системы дистанционного обучения (СДО) университета, то решение данной задачи находится путем комплексного применения методов и моделей выявления текущих и новых киберугроз для СДО и подбора соответствующих контрмер по противодействию этим угрозам.

Задачи исследования:

− проанализировать базовый подход к киберзащите цифровой образовательной среды современных университетов (ЦОСУ) и ее компоненты – системы дистанционного образования (СДО), а также проанализировать вопросы по обеспечению функциональной устойчивости (ФУ) и КБ облачных виртуальных ресурсов (ВОР) СДО;

− разработать модели для описания систем защиты информации СДО;

− усовершенствовать метод выявления киберугроз в СДО;

− усовершенствовать математические модели для обеспечения ФУ и КБ ВОР для программно-конфигурируемых сетей СДО, а также разработать методику обеспечения ФУ и КБ ВОС на основе применения программно-конфигурируемых сетей;

− усовершенствовать методику выбора оптимального варианта построения системы защиты информации и кибербезопасности СДО.

Методы исследований:

В ходе исследования, учитывая особенности предметной области и сформулированных задач, использовались методы: системного анализа и теории сложных систем (для описания иерархической информационной сети СДОУ графом состояний и переходов случайного процесса функционирования); теоретические основы функциональной устойчивости и защищенности информационной сети СДОУ (для моделирования надежности СДО); методы экспертных оценок, комбинаторной теории и аналитического моделирования (для усовершенствования математической модели обеспечения ФУ и КБ ВОР); общие положения теории массового обслуживания и теории игр (для совершенствования методик выбора оптимального варианта построения системы ЗИ и КБ СДО).

Научная новизна исследования:

− разработана модель для описания киберугроз СДО на базе марковских цепей, что позволяет строить конкретные марковские модели угроз атак на ЦОСУ и СДО и в совокупности с моделями, и алгоритмами выбора рациональной стратегией инвестирования в КБ СДО, дает возможность

усовершенствовать методологию построения функционально устойчивой и защищённой СДО;

− усовершенствован метод выявления киберугроз в СДО, который в отличие от существующих, содержит рекурсивные алгоритмы распределенного сетевого самообучения и выбора контрмер (стратегий, в частности финансовых или технических для стороны защиты СДО) в зависимости от вида киберугроз;

− усовершенствована математическая модель для обеспечения ФУ и КБ ВОР для программно-конфигурируемых сетей СДО, которая в отличие от существующих, учитывает состояние ВОР и выбор возможных контрмер на основе комплексного показателя для программно-конфигурируемых сетей, а также за счет процедуры применения графов атак на ВОС, который позволяет получать информацию обо всех известных уязвимостях системы, а также показывает в режиме реального времени состояние ФУ и КБ ВОР;

− получила дальнейшее развитие методика выбора оптимального варианта построения системы ЗИ и КБ СДО, которая в отличие от существующих, дополнена усовершенствованным методом выявления киберугроз в ИнС и СДО, моделью системы управления информационной безопасностью СДО как системы массового обслуживания и моделью антагонистической игры для поиска эффективных и действенных СЗИ в условиях ограниченного бюджета учебного заведения.

Теоретическая значимость исследования: Получили дальнейшее развитие модели и методы защиты систем дистанционного обучения (СДО) в условиях роста сложности деструктивного вмешательства в их работу со стороны компьютерных злоумышленников. При этом впервые была получена модель для описания киберугроз СДО на базе марковских цепей, что позволяет строить конкретные марковские модели угроз атак на СДО. Также усовершенствованы метод выявления киберугроз в СДО, который в отличие от существующих, содержит рекурсивные алгоритмы распределенного сетевого самообучения и модель для обеспечения функциональной устойчивости и кибербезопасности виртуальной облачной среды для программно-конфигурируемых сетей СДО, которая в отличие от существующих, учитывает состояние облачной среды университета и позволяет реализовывать выбор возможных контрмер на основе комплексного показателя для программно-конфигурируемых сетей.

Практическое значение полученных результатов: Разработка прикладных программных продуктов (ПП) в среде Rad Studio 10.3. Разработанные ПП обеспечивают большую эффективность процесса проектирования СУИБ СДО и повышают достоверность результатов интерпретации уровня приемлемого риска для СДО. Проведенные вычислительные эксперименты на базе разработанных программных продуктов подтвердили достоверность основных теоретических положений диссертационной работы. Экспериментально показано, что предложенные решения позволяют повысить показатель ФУ и КБ ВОС, и СДО в целом на 12–17 % по сравнению с известными решениями.

Предложенные методы, модели и разработанные ПП могут быть использованы для повышения степени киберзащищенности СДО университетов.

На защиту выносятся следующие положения:

− модель для описания киберугроз систем дистанционного обучения на базе марковских цепей;

− метод выявления киберугроз в системах дистанционного обучения, содержащий рекурсивные алгоритмы распределенного сетевого самообучения и выбора контрмер в зависимости от вида киберугроз;

− модель для обеспечения функциональной устойчивости и кибербезопасности виртуальных облачных ресурсов для программно-конфигурируемых сетей систем дистанционного обучения;

− методика выбора оптимального варианта построения системы защиты информации и кибербезопасности систем дистанционного обучения.

Личный вклад соискателя: Все основные результаты диссертационной работы, выносимые на защиту, полученные соискателем лично, среди них: модели и алгоритмы обеспечения кибербезопасности виртуальных облачных ресурсов для программно-конфигурируемых сетей системы дистанционного обучения вуза; компьютерная модель системы управления информационной безопасностью дистанционного образования университета как системы массового обслуживания.

Апробация результатов диссертации: Освещена в научном-методическом семинаре «Информатизация образования и проблемы обучения» кафедры информатики и информатизации образования Казахского национального педагогического университета имени Абая, институте «системы управления и информационные технологии» Алматинского университета энергетики и связи, факультете «Информационные технологии» Национального университета биоресурсов и природопользования (Украина), а также на международных научно – методических, практических конференциях: республиканская научно-практическая конференция «Современные информационно-коммуникационные технологии в науке и практике в образовании» (г. Алматы, 2018); республиканская научно-практическая конференция «Цифровые технологии в промышленности» (г. Актау, 2019); международные Сатбаевские чтения «Инновационные технологии – ключ к успешному решению фундаментальных и прикладных проблем в горном и нефтегазовом секторах экономики РК» (г. Алматы, 2019); IX Международная научно-методическая конференция " математическое моделирование и информационные технологии в образовании и науке» (Алматы, 2020); I Международная научно-практическая конференция «Безпека ресурсів інформаційних систем» (Чернигов, 2020).

Также внедрены в учебный процесс в центре «повышение квалификации и дистанционное образование» Казахского национального педагогического университета имени Абая, в институте «систем управления и информационных технологий» Алматинского университета энергетики и

связи, на факультете «информационных технологий» Национального университета биоресурсов и природопользования (Украина).

Публикации по результатам исследования: Основные результаты диссертационной работы опубликованы в 14 научных статьей, в том числе, в журналах входящих в базу Scopus – 3, в журналах рекомендованных КОКСОН МОН РК – 6, в сборниках материалов зарубежных конференций – 1, в материалах международных конференций – 4.

Структура диссертации: Диссертация состоит из введения, трех разделов, заключения, списка использованной литературы и приложений.

Adranova Asselkhan Bagdatovna

Dissertation for the degree of Doctor of Philosophy (PhD) in the specialty 6D060200 – «Informatics» on the theme «Models, methods and algorithms for information security of distance learning»

ANNOTATION

The relevance of research: The increasing scale of the use of new digital technologies in universities, the use of information platforms and systems, in particular cloud ones, in the tasks of distance education, the implementation of innovative hardware and software into the educational process, make the information and educational environment of educational institutions vulnerable against the increasing complexity and the number of destructive attempts of interference in their work. At the same time, we assume that the protected information that is stored and circulated in distance learning systems (DLS) of universities includes: personal data of students, teachers, researchers; digitized information representing the intellectual property of the educational institution; information arrays that provide the educational process (for example, multimedia content, databases, training and other proprietary programs and third-party software products) and etc. The listed information resources in the DLS of the university can act as an object of theft or distortion by external (internal) computer intruders or by hooligan motives of the students or employees.

The formed trend in many post-industrial countries towards the globalization of access to DLS of universities makes relevant the tasks associated with the study of the problems of their more reliable protection and the development of promising cybersecurity strategies (CB) of universities in general.

At the same time, traditional methods for creating DLS protection circuits based on multiple redundancy, the introduction of built-in anti-virus control systems and elements with an increased level of reliability worsen the technical and economic characteristics of the designed and existing distance learning systems. In addition, this approach often does not lead to the necessary reduction in the probability of situations associated with distortion or substitution of content in the DLS of universities, as well as with ensuring the reliability of their work in general.

Information and communication technologies in universities, in particular, DLS, are one of the key elements of the educational process. It should be noted that modern educational institutions, as elements of the political and social sphere, are directly related to information resources and information technologies. The main components of a modern DLS and its information network (InN) are computer technologies, cloud technologies, mobile technologies, information security technologies, technologies of modern data processing centers, etc. They are closely interconnected and, in turn, affect the software and hardware complex Therefore, it becomes necessary to introduce a variety of new innovative solutions that will provide students with a fairly quick access to the IT infrastructure, IT resources of the DLS, on the one hand, and on the other hand, will ensure the functional stability of the work (FS) of the DLS and its CS in real time.

Most of the research in the field of financing information protection systems (IPS) of complex distributed computing networks, which can certainly include DLS, as well as virtual cloud systems (VCS), actively implemented in the educational process, are focused only on the economic problem statement of finding optimal strategies for investing financial resources in the means of CS and IPS. These works, as a rule, do not take into account the trends regarding the introduction of the most advanced information technologies in the control and decision-making procedures for such projects. The disadvantage of many models for the allocation of financial resources spent on the choice of countermeasures for cyber threats in the DLS is the lack of specific recommendations for the formation of strategies of financial investments in the IPS and CS.

Therefore, there is a need for a new research in the direction of the development of methods and models for computer decision support systems, which will make it possible to find optimal strategies for the allocation of limited financial resources of universities to create and maintain functionally stable and cybersecure DLS as a whole.

Many domestic and foreign scientists, in particular: B.S.Akhmetov, R.G. Biyashev, A.B.Barabanov, D.P.Zegzhda, M.N. Kalimoldaev, S.V. Kazmirchuk, A.G. Korchenko, T.S.Kartbaev, V.A. Lakhno, V.V. Malyukov, A.S.Markov, U.A. Tukeyev, M. Atighetchi, R.H. Campbell, J. Dawkins and many others were involved in information protection tasks and in the process of creation of effective information security control systems for various informatization objects. As their studies show, there is a clear contradiction between the fundamental possibility of developing cyber-protected, functionally resistant to attacks and unauthorized access (UAA) DLS of universities, based on the use of information technologies, and the insufficient effectiveness of existing systems for protecting information networks of universities, which do not provide a given level of cybersecurity and functional stability of DLS.

In order to resolve the above contradiction, the dissertation posed a new scientific task, which consists in developing models, methods and information technologies for creating a functionally stable and protected DLS of a university based on existing and promising information networks. Therefore, the topic of the dissertation work, which is aimed at solving this problem, is relevant and is of scientific and practical interest.

The aim of the research: The aim of the dissertation work is to develop models, methods and information technologies used for protecting distance learning systems in conditions of a constant increase in the number of destabilizing effects based on identifying cyber threats and choosing appropriate countermeasures.

The object of the research: The processes of identifying cyber threats and ensuring the functional stability of the DLS.

The subject of the research: The methods and models of ensuring the information security of the DLS of universities.

Research hypothesis: If it is necessary to increase the degree of information protection and cybersecurity of the University's distance learning system, the

solution to this problem is through the integrated application of methods and models for identifying current and new cyber threats to the distance learning system and selecting appropriate countermeasures to counter these threats.

Research objectives:

- to analyze the basic approach to cyber protection of the digital educational environment of modern universities (DEEU) and its components - distance learning systems (DLS), as well as to analyze the tasks of ensuring the functional stability (FS) and CS of virtual cloud resources (VCR) of the DLS;
- to develop models for describing the information security systems of the DLS;
- improve the method for identifying cyber threats in the DLS;
- to improve mathematical models for providing FS and CS of VCR for software-configurable network of the DLS, as well as to develop a methodology for providing FS and CS of VCR based on the use of software- configurable networks;
- to improve the methodology for choosing the optimal variant for creating an information security and cybersecurity system for DLS.

Research methods:

During the research, taking into account the peculiarities of the subject area and the formulated tasks, the following methods were used: system analysis and the theory of complex systems (to describe the hierarchical information network of the DLSU by a graph of states and transitions of a random functioning process); theoretical foundations of the functional stability and security of information network of the DLSU (for modeling the reliability of the DLS); methods of expert assessments, combinatorial theory and analytical modeling (to improve the mathematical model for ensuring FS and CS of VCR); general provisions of the queuing theory and game theory (to improve the methods for choosing the optimal variant for creating a system of IP and CS of the DLS).

Scientific novelty of the research:

− there was obtained a model for describing the cyber threats of the DLS based on Markov chains, which allows creating specific Markov models of attacks on DEEU and DLS, and in conjunction with models and algorithms for choosing a rational strategy for investing of CS of the DLS, makes it possible to improve the methodology for creating a functionally stable and secure DLS;

− *there was improved the method* for identifying cyber threats in the DLS, which, in contrast to the existing ones, contains recursive algorithms for distributed network self-learning and the choice of countermeasures (strategies, in particular financial or technical for the DLS protection), depending on the type of cyber threats;

− *there was improved* a mathematical model for ensuring FS and CS of VCR for software-configurable networks of DLS, which, unlike the existing ones, takes into account the state of VCR and the choice of possible countermeasures based on a complex indicator for software- configurable networks, as well as through the procedure for applying attack graphs on VCS, which allows to receive information

about all known vulnerabilities of the system, and also shows the state of the FS and CS of VCR in real time;

− *there was further developed* the methodology for choosing the optimal variant for creating a system of IP and CS of the DLS, which, in contrast to the existing ones, was supplemented with an improved method for identifying cyber threats in InN and DLS, with a model of an information security control system of the DLS as a queuing system and with an antagonistic game model for finding effective and efficient IPS in conditions of a limited budget of the educational institution.

The theoretical significance of the research: Fact that models and methods for protecting distance learning systems have been further developed in the context of increasing complexity of destructive interference in their work by computer attackers. At the same time, for the first time, a model was obtained for describing cyber threats of a distance learning system based on Markov chains, which allows us to build specific Markov models of threats of attacks on distance learning systems. Also improved method of detecting cyberthreats in distance learning systems, which in contrast to existing, contains, recursive algorithms for distributed network of self-learning and model to ensure the functional stability and cybersecurity virtual cloud environment for software defined networks of the distance learning system, which, unlike existing ones, takes into account the cloud environment of the University and enables the selection of possible countermeasures on the basis of a complex indicator for software defined networking.

The practical significance of the results obtained: Development of applied software products in the Rad Studio 10.3 environment. The developed software programs ensure greater efficiency of the creating of ISCS of the DLS and increase the reliability of the results of interpreting the level of acceptable risk for the DLS. The computational experiments carried out on the basis of the developed software products confirmed the reliability of the main theoretical provisions of the dissertation work. It has been shown experimentally that the proposed solutions make it possible to increase the FS and CS of VCS, and the DLS in general by 12–17% in comparison with the known solutions.

The proposed methods, models and developed software programs can be used to increase the degree of cyber security of the DLS of universities.

The following provisions are brought to the defense:

- a model for describing cyber threats in the distance learning systems based on Markov chains;
- a method for identifying cyber threats in the distance learning systems, containing recursive algorithms for distributed network self-learning and the choice of countermeasures depending on the type of cyber threats;
- a model for ensuring the functional stability and cybersecurity of virtual cloud resources for software-configurable networks of distance learning systems;
- a methodology for choosing the optimal variant for creating an information security and cybersecurity system for the distance learning systems.

Personal contribution: All the main results of the dissertation work for the defense, received by the doctoral student personally, among them: *models and algorithms* for ensuring cybersecurity of virtual cloud resources for software-configurable networks of the university's distance learning system; *computer model* of the information security control system of the distance learning of the university as a queuing system.

Approbation of the dissertation results: Presented of the scientific and methodical seminar «Informatization of education and the problem of education» of the Kazakh National Pedagogical University named after Abay (Kazakhstan), the Department "Control Systems and Information Technologies" of the Almaty University of Energy and Communications (Kazakhstan), the Faculty of "Information Technologies" of the National University of Bioresources and Nature Management (Ukraine), and also at international scientific – methodical, practical conferences: republican scientific and practical conference "Modern information and communication technologies in science and in practice in education" (Almaty, 2018); republican scientific and practical conference "Digital technologies in industry" (Aktau, 2019); international Satpayev readings "Innovative technologies are the key to successfully solving fundamental and applied problems in the mining and oil and gas sectors of the economy of the Republic of Kazakhstan" (Almaty, 2019); IX international scientific and methodical conference "Mathematical modeling and information technologies in education and science" (Almaty, 2020); I international scientific and practical conference "Security of information systems resources" (Chernihiv, 2020).

They are also implemented in the educational process at the center " Excellence and Distance Education" of the Abay Kazakh national pedagogical University, at the Institute of "management systems and information technologies" of the Almaty University of energy and communications, at the faculty of "information technologies" of the National University of bioresources and environmental management (Ukraine).

Research publications: The main results of the dissertation work were published in 14 printed works, including 3 articles in journals included in the Scopus database, 6 articles in journals recommended by the CQAES MES RK; 1 publications in materials of foreign conferences, 4 publications in materials of international conferences.

Dissertation work structure: The dissertation consists of an introduction, three chapters, a conclusion, a list of references and appendices.