6D070400 – «Есептеу техникасы мен бағдарламалық қамтамасыз ету» мамандығы бойынша (PhD) философия докторы дәрежесін алу үшін дайындалған Бекетова Гулжанат Сакитжановнаның «Аса маңызды компьютерлік жүйелерде кибер қаупін интеллектуалды тану моделдері мен әдістері» тақырыбындағы диссертациялық жұмысына ресми пікір берушінің

СЫН-ПІКІРІ

1. Зерттеу тақырыбының өзектілігі және оның жалпы ғылыми, мемлекеттік бағдарламамен байланысы (практиканың және ғылым мен техника дамуының сұраныстары)

Критикалық маңызды компьютерлік жүйелерді қолдану салаларының, әсіресе мобильдік, таратылған және сымсыз ақпараттық технологиялар сегменттерінде белсенді кеңеюі ақпараттық қауіпсіздік үшін жаңа қауіптердің туындауымен бірге жүреді. Бұл критикалық маңызды компьютерлік жүйелердің кибер қорғауға және ақпараттық қауіпсіздікке байланысты инциденттері, сонымен бірге олардың программалық қамсыздандыруында анықталған әлсіз тұстары санының өсуімен көрсетіледі. Қауіптер өте нақты, сондықтан қылмыскерлер құпиясөздерге, жеке файлдарға, геолокациялық ақпараттарға ене алады, аудио- және видео мәліметтерді тарата алады, Wi-Fi желілерін, веб-камераларды, ақпараттық таблоларды және тағы басқаларын басқара алады. Мәселенің қауіптілігі туралы бірнеше рет орын алған зиянкестердің әрекеттері бойынша, яғни бір немесе бірнеше зиянкес тұлғалардың критикалық маңызды компьютерлік жүйелердің мәліметтеріне еніп, аз ғана уақыт ішінде ірі компаниялардың жұмысын толығымен тоқтатуын айтуға болады.

Демек, критикалық маңызды компьютерлік жүйелердің қауіптерін интеллектуалды тану негізінде қорғау модельдері мен әдістерінің одан әрі дамуына бағытталған зерттеудің өзектілігі мемлекеттің критикалық инфрақұрылымын киберқорғаудың негізгі проблемаларының бірі болып табылады. Бұл проблемалардың маңыздылығы критикалық маңызды компьютерлік жүйелердің ұлттық қауіпсіздік пен мемлекеттің экономикасымен, потенциалды әлсіздіктерімен, ол кибер шабуылдың жаңа кластарының пайда болуымен, сымсыз коммуникацияның кең таралуымен, GPS, ГЛОНАСС, GALILEO-ны қолдану навигация жүйесімен, бейне бақылау жүйесімен, GSM, VSAT байланыс технологиясымен, PLC диспетчерлік басқару жүйесімен (SCADA, HMI) шартталған.

2. Диссертацияға қойылатын талап деңгейіндегі ғылыми нәтижелері (п.п. 2,5,6 «Ғылыми дәрежелерін беру ережелері»)

Диссертациялық жұмыс зерттеліп отырған салаға қатысты сұрақтарға жасалған талдауларды қамтитын, өзекті бағыттарды зерттеу мен қол жеткізген ғылыми нәтижелерге негізделген біртұтас ғылыми зерттеулер болып табылады. Диссертация кіріспеден 4-бөлімнен, қорытындыдан, пайдаланылған әдебиеттер тізімі мен қосымшалардан тұрады.

Кіріспеде зерттеудің өзектілігі, зерттеу мәселесіне байланысты

проблемалар нақтыланды. Жұмыстың идеялары, зерттеудің мақсаттары мен міндеттері, жұмыстың ғылыми жаңылықтары мен практикалық бағалығы келтірілген.

Бірінші бөлімде критикалық маңызды компьютерлік жүйелерге кибер шабуылдың кластары мен типтері қарастырылған, алдыңғы зерттеулерге шолу мен талдау жасалды, сонымен бірге танудың интеллектуалды технологиялары негізінде шабуылды тану жүйелері синтезі бағытында жұмыстар жүргізілді.

Екінші бөлімде критикалық маңызды компьютерлік жүйелердің (КМКЖ) ақпараттарын интеллектуалды адаптивті қорғау компоненттерін қолдану кибер шабуылдар үшін элементар классификатор түсінігі мен логикалық процедуралар қолдануға негізделу мүмкіндігі көрсетілді. Кластар мен элементар классификатор қабатын құруға негізделген КМКЖ-лерде кибер шабуылдарды іздеу моделі ұсынылды. Логикалық функциялардың аппаратын қолдана отырып шабуылдарды танудың логикалық процедураларын құрудың негізгі қадамдары көрсетілген. Белгілі бір кластар аясында, қателердің минималды санымен шабуылдарды танудың логикалық процедуралары үшін ережелерді құру әдіснамасы өңделді.

Үшінші бөлімде КМКЖ-ге арналған ақпараттық қауіпсіздік жүйесі кешендері құрамын оңтайландыру есептерін шешу үшін қолданылатын модельдерге нақтылаулар ұсынылды. Бұл нақтылаулар КМКЖ-ң ақпараттық қауіпсіздік жүйесін критикалық және критикалық емес құрамдас бөліктерге алдын-ала декомпозициялау аспектісіне қатысты және осы мақсатта резервтік көшірме алу процедурасы қарастырылды. КМКЖ ақпараттық қауіпсіздік жүйесі кешендері құрамын оңтайландыру есептері қарастырылған. КМКЖ-ге арналған ақпараттық және программалық массивтердің құрылымдық-технологиялық сақтық қорын оңтайландыру моделі нақтыланды және КМКЖ кибер қауіпсіздігін қамтамасыз ету есебін шешу үшін дискретті оңтайландыру әдісін қолдану ерекшеліктері қарастырылды.

Төртінші бөлімде КМКЖ-ге шабуылдаушы жақтың кибер шабуылдардың әр түрлі сценарийлерін беруде жүйенің ықтимал жағдайын сипаттайтын модельдерді беру үшін MATLAB және Simulink орталарында өзіндік модульдерді жазу мен қосу мүмкіндіктері талданды. MATLAB және Simulink-те өңделген модельдердің КМКЖ модульдеріне кибер шабуылды имитациялық модельдеу есебінен кибер қорғау жүйесі жобасын ретке келтіру уақытын 25-30%-ға азайтуға мүмкіндік беретіндігі көрсетілген.

Қорытындыда диссертациялық жұмыстың негізгі нәтижелері мен зерттеу нәтижелерінің практикалық қолданылуы туралы ақпараттар көрсетілген.

3. Ізденушінің диссертацияда келтірілген нәтижесінің, түйіндемесінің және қорытындысының түсініктемелік және дәлелдік деңгейлік дәрежесі

Диссертациялық жұмыстың нәтижелері критикалық маңызды компьютерлік жүйелердің кибер қорғау жүйесін құру мәселесіне арналған

жоба-құрастырымдық және ғылыми-зерттеу ұйымдарында, сонымен бірге жоғары оқу орындарында қолданылады.

Ғылыми нәтижелердің анықтығы мен негізділігі 1) өңделген модельдердің математикалық дұрыстылығымен; 2) критикалық маңызды компьютерлік жүйелердің кибер шабуылдарды интеллектуалды тану моделінің теориялық және практикалық анықтылығымен; 3) критикалық маңызды компьютерлік жүйелердің кибер шабуылдарды интеллектуалды тану үшін экспертті жүйелерді практикалық ендірумен; 4) критикалық маңызды компьютерлік жүйелерге шабуылды тестілеу мен кибер шабуылдарды имитациялық модельдеу нәтижелерімен сәйкес келуімен бекітілген.

4. Ізденушінің диссертацияда тұжырымдалған әрбір нәтижесінің түйіндемесінің және қорытындыларының жаңалығының дәрежесі

Диссертациялық зерттеуді орындау аясында төмендегідей ғылыми зерттеулер алынды:

1. Алғаш рет өңделді:

- қауіп, ауытқу мен кибер шабуылдар кластары үшін белгілердің бинарлық ақпаратталған сипаттамаларын құратын матрицалар қабаты бойынша конъюнкцияның анықталуына негізделетін киберқауіптерді интеллектуалды тану әдісі. Аталмыш әдіс басқалардан логикалық функцияларды және кибер шабуылдар белгілерінің анық емес жиындарын қолдану арқылы ерекшеленеді, ал бұл критикалық маңызды компьютерлік жүйелер үшін ақпаратты қорғау жүйелерінің тиімді аналитикалық, сызбатехникалық және программалық шешімдерін құруға мүмкіндік береді;
- критикалық маңызды компьютерлік жүйелердің жеке компоненттерінің критикалығына талдау жасау процедурасына, бинарлы белгілер матрицасы қабаты мен элементар классификатор түсінігіне негізделген кибер шабуылдарды сәйкестендірудің логикалық процедуралары үшін шешуші ережелерді қалыптастыру және тану моделі, басқа белгілі модельдерден ерекшелігі, қателердің аз санымен интеллектуалды тану мүмкіндігі.

2. Жетілдірілді:

- құрылымды-технологиялық және виртуалды-қалпына келу сақтық қорының, сонымен бірге критикалық маңызды компьютерлік жүйелердің программалық-ақпараттық қамтамасының оңтайландыру моделі. Бұл модельдер басқаларынан шабуылдаушы жақтың әрекетімен қауіпті, ауытқуды және кибер шабуылды тану жүйесін кедергілердің максималды ықтималдық критериясын қолдануымен ерекшеленеді, ол жобалау этабында кибер шабуылдың түрлі кластарына ақпараттық қауіпсіздік жүйелерінің функционалдылығы мен тұрақтылығын бағалауға мүмкіндік береді.

3. Ары қарай дамытылды:

- критикалық маңызды компьютерлік жүйелерге төнетін кибер шабуылдардың күрделі, комбинацияланған түрлеріне талдау жасауға, кедергі келтіру мен одан болған зардаптарды бейтараптандырудың рационалды тәсілдерін таңдауға мүмкіндік беретін критикалық маңызды компьютерлік жүйелердің элементтеріне кибер шабуылдың имитациялық моделі.

5. Алынған нәтижелердің ішкі бірлігін бағалау

Диссертациялық зерттулерде алынған ғылыми нәтижелер олар біріңғай есептерді шешімі болғандықтан ішкі біртұтастыққа ие. Бұл біртұтастық дәрежесі әрбір алынған нәтиже алдыңғысының салдары болғандықтан жоғары болады.

6. Ізденушінің алған нәтижелерінің тиісті өзекті мәселені, теориялық немесе қолданбалы міндетті шешуге бағытталғандығы

Жүргізілген зерттеу өзекті, ториялық және қолданбалы мәнге ие. Зерттеу нәтижелері Қызылорда қаласындағы Қорқыт Ата атындағы Қызылорда мемлекеттік университетінің «Есептеу техникасы және ақпараттық жүйелер» кафедрасының, Ұлттық авиациялық университетінде (Киев қаласы, Украина) «Ақпараттық технологиялар қауіпсіздігі» кафедраларының оқу үдерісінде қолданылды. Сонымен қатар жұмыстың нәтижелері «Сайфер БИС» ЖШҚ-ның (Украина, Киев қаласы), «QUARES» (Алматы қаласы) ЖШС-ның жұмыстарына ендірілген. Ерекше айта кететіні, диссертациялық жұмысты Орталық Азия және Моңғолия елдеріндегі Касперский Зертханасы ЖШС-нің басқарушы директоры Е.В.Питолин жоғары бағалады.

7. Негізгі ережелері, нәтижелері мен қорытындылары жарияланған басылымдарының толықтылығының жеткіліктілігін растау (п.7 ғылыми дәрежелерін беру ережелеріне сәйкес)

Диссертация тақырыбы бойынша 21 жұмыс жарияланған, оның 8 – ҚР БҒМ Білім және ғылым саласындағы бақылау комитеті ұсынған басылымдарда жарияланған, 3 мақала Scopus мәліметтер қорына кіретін басылымда жарияланған, 1 мақала шетелдік журналда жарияланған, 9 мақала халықаралық ғылыми-тәжірибелік конференция жинақтарында жарияланған.

8. Аңдатпаның диссертация жұмысына сәйкестілігі

Диссертациялық жұмыстың аңдатпасы диссертация мазмұнына толық сәйкес келеді.

9. Диссертация мазмұны мен дайындау бойынша кемшіліктері

Диссертациялық жұмысқа, оның ерекшеліктеріне қарамастан, келесі ескертулер жасалады:

1. Жұмыста кибер шабуылдың бір класына арналған элементар классификаторларды қалыптастыру, сондай-ақ қауіптің, ауытқулардың және шабуылдардың барлық белгілі кластары үшін пайдаланылатын жиындардың өлшемі көрсетілмеген. Бұл сұрақты ізденуші ашық түсіндіру қажет.
2. Жұмыста имитациялық модельдерді құру үшін Simulink бағдарламасының 6.0 нұсқасы пайдаланғаны көрсетілген. Қазіргі уақытта 8.8 нұсқасы бар. Зерттеудің практикалық маңыздылығын ескере отырып, модельдеуді жүргізу үшін Simulink бағдарламасының соңғы нұсқасын қолданғаны жөн.
3. Жұмыста КМКЖ қауіптерін тану үшін білім базасының толық сипаттамасы көрсетілмеген. Мәтіннен «белгілердің ақпараттылығы» параметрі үшін сандық мәндер қалай таңдалғаны түсініксіз.

Көрсетілген кемшіліктер зерттеу сапасын төмендетпейді және диссертацияның теориялық және практикалық нәтижелеріне әсер етпейді.

10. Диссертацияның «Ғылыми дәрежелер беру ережелерінде» қойылған талаптарға сай келуі

Қорытындылай келе, «Аса маңызды компьютерлік жүйелерде кибер қаупін интеллектуалды тану моделдері мен әдістері» тақырыбындағы диссертациялық жұмыс аяқталған ғылыми зерттеу жұмысы болып табылады, қойылған мақсатқа жетуде маңызды ғылыми-әдіснамалық қадам ретінде ерекшеленеді.

Диссертациялық жұмыс «Ғылыми дәрежені беру ережесінің» талаптарына сай, ал оның авторы Бекетова Гулжанат Сакитжановна 6D070400 – «Есептеу техникасы мен бағдарламалық қамтамасыз ету» мамандығы бойынша философия докторы (PhD) ғылыми дәрежесін алуға лайық деп есептеймін.

Рецензент
ф.-м.ғ.к., доцент
Алматы энергетика және байланыс университеті **А.У. Калижанова**

Персоналды басқару жөніндегі бөлім
Отдел по управлению персоналом

Қолтаңбаны растаймын
Подпись заверяю
Бөлім бастығы Д. Капанова
«08» 12 2017 ж.