6D070400 – «Есептеу техникасы мен бағдарламалық қамтамасыз ету» мамандығының PhD докторанты Г.С.Бекетованың «Аса маңызды компьютерлік жүйелерде кибер қаупін интеллектуалды тану моделдері мен әдістері» тақырыбындағы диссертациялық жұмысына

АҢДАТПА

Зерттеудің өзектілігі. Компьютерлік жүйелер мен ақпараттық-коммуникациялық технологиялардың бірлескен қолданылуы еңбектің өнімділігін арттыруға, материалды-шикізаттық шығындарды азайтуға және өнім сапасы мен өмір сүру деңгейін жақсартуға септігін тигізеді. Компьютерлік жүйелер мен ақпараттық технологиялар тұтынушыларға энергия ресурстарын, суды, тамақ өнімдерін уақытында жеткізу, көлік пен байланыс қызметтерін беруге жауапты критикалық маңызды инфрақұрылымның эксплуатациясы мен техникалық қызмет көрсетілуінде маңызды рөл атқарады. Осындай критикалық маңызды инфрақұрылымның маңызды элементі компьютерленген жүйелер болып табылады. Жұмысының бұзылуы мемлекеттің немесе жеке аймақтардың масштабында айтарлықтай тіпті өте қауіпті әлеуметтік және экономикалық зардаптарға алып келеді, ол критикалық маңызды компьютерлік жүйелердің әртүрлі компоненттері мен тіршілікті қамтамасыз ету кешендері арасында күшті жүйелік өзара байланыспен шартталады. Критикалық маңызды компьютерлік жүйелердің жоғары жұмысқа қабілеттігін, сенімділігін және қауіпсіздігін кепілдендіру үшін олардың ақпараттық қауіпсіздігімен және киберқорғауымен байланысты мәселелерін алдын ала шешу қажет.

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.

Осылайша, 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.

Зерттеу мақсаты мен міндеттері. Диссертациялық жұмыстың мақсаты ақпараттың құпиялылығы, тұтастығы мен қол жетімдігіне тұрақсыздандырушы

әсер санының үнемі өсуі жағдайында кибер қауіпті интеллектуалды тану негізінде критикалық маңызды компьютерлік жүйелерді қорғау модельдері мен әдістерінің дамуы болып табылады.

Қойылған мақсаттарға жету үшін төмендегі міндеттерді шешу қажет:

1. Критикалық маңызды компьютерлік жүйелердің кибер шабуылдарға орнықтылығын арттыру үшін киберқорғаудың инновациялық интеллектуалды жүйесін қолдану негізінде критикалық маңызды компьютерлік жүйелер киберқауіпсіздігін қамтамасыз етуге мүмкіндік беретін кауіп, ауытқу және кибер шабуылды интеллектуалды тану әдісін өңдеу.

2. Белгілер матрицасы қабатына және элементар классификатор түсінігіне негізделген ауытқу мен кибер шабуылды анықтаудың логикалық процедураларын қолданып интеллектуалды тану моделін өңдеу.

3. Қауіп, ауытқу және кибер шабуылды танудың интеллектуалды жүйесінің репозиториінде орналасқан белгілер үшін үйретуші іріктемелер санын азайту.

4. Ақпараттық қауіпсіздік деңгейін жоғарылату үшін критикалық маңызды компьютерлік жүйелер модулдерінің аса маңыздылығын есепке ала отырып оның программалық және ақпараттық қамсыздандыруының құрылымды-технологиялық сақтық қорын анықтау моделін, сонымен қатар оның критикалық маңызды компьютерлік жүйелердің функционалды параметрлеріне әсері есебімен ақпаратты қорғау жүйелерінің рационалды құрылымын таңдауға мүмкіндік беретін модельді жетілдіру.

5. Критикалық маңызды компьютерлік жүйелердің негізгі компоненттерін және ондағы қауіптер, ауытқулар және кибер шабуылдарды интеллектуалды танудың ұсынылған модельдеріне негізделген киберқорғаудың ішкі жүйелерін имитациялық модельдеуді орындау.

Зерттеу объектісі – критикалық маңызды компьютерлік жүйелер үшін кибер шабуылдарды интеллектуалды тану үдерісі.

Зерттеу пәні – критикалық маңызды компьютерлік жүйелерді қорғаудың әдістері мен модельдері.

Зерттеу әдістері. Зерттеу барысында, пәндік аймақ пен қалыптасқан міндеттердің ерекшеліктерін ескере отырып, төмендегілер қолданылды: интеллектуалды тану мен ауытқуларды, кибер шабуылдарды және киберқауіптерді анықтау модельдерін өңдеу үшін бульдік алгебра және анық емес жиындар теориясы; критикалық маңызды компьютерлік жүйелердің кибер қорғауын қамтамасыз ететін есептерді тиімді шешу үшін дискретті оңтайландыру әдісі; өңделген модельдердің жүзеге асырылуы үшін имитациялық модельдеудің әдістері мен құралдары; қолданбалы программалық өнім құру үшін объектіге-бағытталған программалаудың принциптері мен әдістері.

Зерттеу нәтижелерінің ғылыми жаңалықтары. Диссертациялық зерттеуді орындау аясында төмендегідей ғылыми зерттеулер алынды:

1. 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.

Диссертацияның талаптары аясында ғылыми нәтижелер.

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 төнетін кибер шабуылдарды зерттеуге арналған ғылыми еңбектеріне талдау жүргізілген. 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.

Зерттеу нәтижелерінің апробациясы

Зерттеудің негізгі нәтижелері Қ.И.Сәтбаев атындағы ҚазҰТЗУ-дың «Компьютерлік және программалық инженерия» кафедрасының және Ұлттық авиациялық университетінің (Киев қаласы, Украина) «Ақпараттық технологиялар қауіпсіздік» кафедрасының ғылыми семинарларында талқыланды, сонымен бірге төмендегі конференцияларда баяндалды: «Қазақстанның жаңа экономикалық саясатын таратуда жас ғалымдардың орны мен рөлі» халықаралық Сәтбаев оқулары (Алматы қ-сы, 2015); «Кибер қауіпсіздік пен ақпаратты қорғауды қамтамасыз етудің өзекті мәселелері» II халықаралық ғылыми-практикалық конференция (Киев қ-сы, 2016); ITSEC халықаралық ғылыми-практикалық конференция (Киев қ-сы, 2016); «Ақпараттық-телекоммуникациялық жүйелердің қауіпсіздігінің жағдайы мен дамуы» халықаралық ғылыми-практикалық конференция SITS-2016 (Украина, Коблево қ-сы, 2016); «Транспортта, өнеркәсіпте және білім берудегі қазіргі ақпараттық және коммуникациялық технологиялар» халықаралық ғылыми-практикалық конференция, (Днепро қ-сы, 2016); «Энергия және ресурстар нгнемдеу технологиялары: тәжірибелер және келешегі» халықаралық ғылыми-тәжірибелік online конференциясы (Қызылорда қ-сы, 2017); «Ғылым, білім және өндіріс интеграциясы – Ұлт жоспарын іске асырудың негізі» Халықаралық ғылыми-практикалық конференциясы, №9 Сағынов оқулары (Қарағанды қ-сы, 2017).

Диссертация Қ.Сәтбаев атындағы ҚазҰТЗУ ақпараттық және телекоммуникациялық технологиялар институтының компьютерлік және программалық инженерия кафедрасында орындалды.

Басылымдар. 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.

Диссертацияның құрылымы мен көлемі. Диссертациялық жұмыс, кіріспеден, төрт бөлімнен, қорытындыдан, 90 пайдаланылған әдебиеттер тізімінен тұрады; барлығы 135 бетте көрсетілген, 64 суреттен, 14 кестеден және 2 қосымшадан тұрады.