6D070400 – «Есептеуіш техника және бағдарламалық қамтамасыз ету» мамандығы бойынша (PhD) философия докторы дәрежесін алу үшін Жумангалиева Назым Кенжегалиеваның «Шабуылдарды табу жүйесіне арналған параметрлер күйінің ауытқымалығын бақылау технологиясы» тақырыбындағы диссертациялық жұмысына ресми пікір берушінің

СЫН-ПІКІРІ

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

Интернеттің қарқынды дамуы, ақпаратты сақтау және тасымалдаудың электронды нысандарына көшіру, электронды төлем түрлерін күнделікті өмірге белсенді енгізу және басқа да көптеген факторлар бүгінгі күннің өзінде барлық ұйымдар үшін желілер мен желілік қызметтердің қауіпсіздігі нақты проблемаға айналды.

Ақпараттық жүйелерге шабуылдардың жалпы санының артуымен ұдайы жаңа шабуылдардың түрлері тұрақты түрде пайда болып, ақпаратты қорғауға қосымша ретінде шабуылдарды табудың және оларға жауап берудің икемді құралдарын пайдалануды қажет етеді.

Кәзіргі таңда қоғамның барлық салаларындағы заманауи компьютерлік технологияларды қолдану үлкен деректер көлемін автоматтандырылған түрде өңдеуге мүмкіндік берді. Қоғамның жаппай компьютерлендіруі пайдаланушылардың кең ауқымына ақпаратпен жұмыс істеуіне мүмкіндік берді. Сонымен қатар, ол түрлі ақпараттық қорларға рұқсатсыз қол жеткізу мүмкіндігін көбейтті. Бұл жаңа кибер шабуылдар туындататын ақпараттық жүйелер қорларына енетін қауіп-қатердің жаңа түрлерінің пайда болуына байланысты теріс әсер етеді.

Ақпараттық жүйелер қорларының кең таралған қауіпсіздік шешімі ретінде ең алдымен компьютерлік желілер арқылы рұқсатсыз қолжеткізуді анықтау фактілеріне бағдарламалық немесе бағдарламалық – аппараттық құралдарға негізделген шабуылдарды анықтау жүйесі болып табылады.

Жұмыстың өзектілігі Қазақстан Республикасының Президентінің 2017 жылғы 15 ақпандағы № 422 «2017 жылғы 31 қаңтардағы Қазақстан халқына Жолдауын іске асыру жөніндегі шаралар туралы», «Қазақстанды үшінші жаңғырту: жаһандық бәсекеге қабілеттілік» туралы Жарлығын іске асыру мақсатында, Киберқауіпсіздік концепциясы («Қазақстан киберщиті») аясында ақпараттық қауіпсіздікті қамтамасыз ету, осы саладағы жағдайларды алдын алу және салаларын азайту мақсатында жасалынғанын атап айтсақ болады.

Диссертациялық жұмыстың тақырыбының өзектілігін желілік сигнатуралық емес кибершабуылдар туындайтын анық емес жағдайда ауытқуды анықтау жүйесінің технология, әдіс, моделі негізінде қазіргі

заманғы шабуылдарды анықтау жүйесінің мүмкіндіктерін кеңейтетін құралдарды өңдеу қажеттілігімен анықталады.

2. Диссертацияларға қойылатын талап деңгейдегі ғылыми нәтижелері

Жумангалиева Н.К диссертациялық жұмысында келесі ғылыми жаңалықтарды атауға болады:

1. Белгілі бір желілік шабуылдардың жиынтығына тән, анық емес айнымалы эталондарын құру үрдісін қалыптастыруға мүмкіндік беретін және қоршаған ортадағы ауытқу жағдайын өлшемін көрсеттін «шабуыл: түйіндес жұп жиынтығы» және «шабуыл: шамалар» жұп жиынтығының негізінде ендірілген шамалардың моделін ұсынылған;

2. Компьютерлік желілердегі ауытқу жағдайын сарапшылық жолмен анықтауға арналған шешуші ережелер жиынын қалыптастыру мүмкінді ұсынылған;

3. Эталонды шамалар жиынының есебінен түйіндес жұп пен анық емес сәйкестендіру матрицасын сарапшылық бағалаудың әдістерімен қалыптасқан шешуші ережелер моделін ары қарай дамытылған;

4. Алғаш рет базалық шамалар моделі мен эталонды шамалар моделі негізінде лингвистикалық бағалау сәйкестендіргіштерінің жиынын және интервалдар сәйкестендіргіштерін қолдану, шамалардың шабуылдарға қатысты ағымдағы жағдайын сипаттайтын сарапшылар пайымдарын бейнелейтін әдісі құрылған;

5.Базалық шамалар, эталонды шамалар және шешуші ережелер моделі негізінде тіркелмеген әрекеттері табу, сарапшылық ұстаным негізінде және қалыптасқан анық емес ағымдағы шамалар арқылы кибершабуылдардың сигнатуралық емес түрлерін сәйкестендіру құралдарын құруға мүмкіндік беретін ауытқу жағдайлардын анықтау технологиясы құрылған;

6. Анық емес арифметика модулі және ішкі жүйелердің есебінен ауытқушылық жағдайын анықтау технологиясының көмегімен жүзеге асырылған шабуылдарды анықтау жүйесінің құрылымдық шешімі қазіргі заманғы жүйесінің функционалды мүмкіндіктерін ары қарай дамытылған.

3. Ізденушінің диссертацияда келтірілген әрбір нәтижесінің, түйіндемесінің және қортындыларының түсініктемелік және дәлділік дәрежесі

Зерттеушінің диссертациялық жұмысында алынған әрбір ғылыми натижелері теориялық жағынан негізделіп, есептеу сараптама арқылы практикалық кундылығы жағынан дәлелденген. Зерттеудің теориялық және әдіснамалық негздері мемлекеттік багдарламаларға және ғылыми теорияларға негізделіп, қарастырылып отырған ғылыми мәселенің зерттелу деңгейін нақтылады. Алынған нәтижелер отандық және шетелдік ғалымдардың ой-пікірлерін саралап талдау нәтижесінде қойылған есептерді шешу мақсатында қолдануға тиімді әдістерге негізделген.

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

Ізденушінің диссертацияда тұжырымдалған әрбір қорытындысы нақты әдістер мен технологияларға негізделіп жаңа нәтижелерге қол жеткізген:

1. Сапалық және сандық әдістердің кең спектірін негізге шабуылдарды анықтау жүйесін құрылған және олардың сараптамасы жүргізілген.

2. Нақты гетереогенді параметрлі ортасында түрлі ауытқушылық жағдайын сипаттайтын, берілген лингвистикалық айнымалылар топтарының шамаларының эталонды мәндерін алу процедурасын қалыптастыруға мүмкіндік беретін, тұңғыш рет шабуылдарды анықтау жүйесі үшін лингвистикалық эталондарды қалыптастыру әдісі құрастырылған.

3. Желілік шамаларының анық емес эталондарын қалыптастырудың ішкі жүйесінің және желілік белсенділікті бағалауға арналған шешуші ережелердің негізінде және сонымен бірге базалық шамалар моделін есепке ала отырып желілік қауіпсіздік жүесін жетілдіруде қолданыла алатын ауытқушылық жағдайын анықтау технологиясын жүзеге асыратын жаңа құрылымдық шешім құрастырылған.

4. Құрастырылған құрылымдық шешімдер мен алгоритмдер негізінде шабуылдаушы әрекеттердің нақты түрлері туындатқан ауытқушылықтарды анықтауға арналған өспелі мүмкіндіктері бар қолданбалы бағдарламалық жүйе құрылған.

5. Алынған нәтижелердің ішкі бірлігін бағалау

Зерттеушінің жұмысы кіріспеден, төрт бөлімнен, қортындыдан, пайдаланылған әдебиеттерден тұрады. Диссертациялық жумыстын бөлімдері бір-бірімен өзара тығыз байланыста қарастарылған. Зерттеу жумысының нәтижесінде жасалған қорытындылар жеке бөлімдердің жалпы мазмұнына үйлесе жасалған, олардьщ ішінде магыналық байланысы сақталған.

Диссертациялық жұмыстағы материал логикалық тұрғыдан жүйелі, зерттеу әдістері мен алынған нәтижелері, қортындылары мен ғылыми түйіндері толық аяқталған және аталған жұмыс квалификациялық ғылыми еңбек екендігін дәлелдейді.

6. Ізденушімен алынған нәтижелерінің өзекті мәселелер, теориялық және тәжірибелік мәселелерді шешуге бағыттылығы

Зерттеудің теориялық және тәжірибелік маңызы байланыс саласында өте жоғары. Ғылыми нәтижелер арқылы компьютерлік желілердегі шабуылдаушы әрекеттерді анықтауға мүмкіндік беретін жаңа техникалық шешімдерді әзірлеу және эксперименталды зерттеу жолдары қарастырылған.

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

Диссертациялық жұмыс бойынша 23 мақала жарияланған, оның ішінде 4 мақала Scopus халықаралық деректер қорына кіреді 8 мақала БҒСБК журналдарына кіреді, 4 мақала шетелдік журналдарда жарияланған, 7 мақала

шетелдік халықаралық ғылыми - тәжірибелік конференция жинақтарында жарияланған олар диссертация тақырыбына, мазмұнына және қорытындысына сәйкес келеді.

8. Аннотацияның диссертациялық жұмысына сәйкестігі

Диссертациялық жұмыс бойынша аннотация диссертация мазмұнына толық сәйкес келеді.

9. Диссертация мазмұны және дайындығы бойынша кемшіліктері

1. Стандарттар мен эвристикалық ережелерді қалыптастыруға арналған сараптамалық тәсілді қолданғанда, автор сарапшылардың пікірлері мен олардың құзыреттілігінің деңгейі сияқты факторларды ескермеген.

2. Желілік мәндердің нақты емес эталонындарын қалыптастыру ішжүйесінің сипаттамасында, оның құрамына «..рұқсатсыз жүйеге ену мен мәндердің идентификаторының ағымдағы өлшемдерін қабылдау және сақтау үшін арналған рұқсатсыз жүйеге енулер мен мәндер (RGIV)» кіреді. Регистрде рұқсатсыз жүйеге енулер емес оның идентификаторлары сақталатынын ескерсек, онда сол регистрді рұқсатсыз жүйеге ену мен мәндер идентификаторларының регистрі деп айтсақ дұрыс болар еді.

3. Аса маңызды емес грамматикалық қателер кездеседі, қазақ тілінде сөздердің қате аудармалары кездеседі.

4. Диссертациялық жұмыста қабылдау қабілеті қиынға соғатын күрделі сөйлемдер кездеседі.

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

Ізденушінің «Шабуылдарды табу жүйесіне арналған параметрлер күйінің ауытқымалығын бақылау технологиясы» тақырыбында жазылған диссертацияда көрсетілген кемшіліктер мен ескертулерге қарамастан аяқталған ғылыми зерттеу жұмысы екендігін көрсетеді, нәтижелері күмәнсіз дұрыс, олар түрлі ғылыми-тәжірибелік конференцияларда баяндалып, жарияланған және мекемеге ендірілген.

Қорытындылай келе, Жумангалиева Назым Кенжегалиевна «Шабуылдарды табу жүйесіне арналған параметрлер күйінің ауытқымалығын бақылау технологиясы» атты диссертациялық жұмысы 6D070400 – «Есептеуіш техника және бағдарламалық қамтамасыз ету» мамандығының (PhD) философия докторы дәрежесін алуға қойылған диссертациялық жұмыстың талаптарына сай және автор осы саланың PhD философия докторы дәрежесін алуға лайықты деп есептеймін.

Рецензент **Сейлова Нургуль Абдуллдаевна**
т.ғ.к., ассистент-профессор,
«Ақпараттық қауіпсіздік» кафедрасының меңгерушісі,
Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

КАДРЛАР БӨЛІМІ

ДҰРЫС
КАДРЛАР БӨЛІМІНІҢ
МАМАНЫ
Күні «08» 12 2017 ж.