**«6D070400- Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығының PhD докторанты Жумангалиева Назым Кенжегалиевнаның «Шабуылдарды табу жүйесіне арналған параметрлер күйінің ауытқымалығын бақылау технологиясы» тақырыбындағы диссертациялық жұмысына**

# АҢДАТПА


**Тақырыптың өзектілігі.** Ақпараттық жүйе ресурстарына шабуылдаушы әрекеттер олардың қоршаған ортасына әсер етеді және белгілі ауытқушылықтар тудырады. Осындай орта әдетте әлсіз қалыптасқан, анық емес және күдікті белсенділікті анықтау үшін арнайы модельдер, әдістер мен жүйелер қолдану қажет. Компьютерлік жүйелердегі басып кірулерді анықтау үшін қолданылатын қазіргі заманғы теориялық және тәжірибелік базаның айқындалмаған, әлсіз қалыптасқан ортада сигнатуралық емес және кибершабуылдардың жаңа түрін айқындау мүмкіндіктеріне қатысты белгілі шектеулер бар. Шабуылдаушы әрекеттер тудырған ауытқушылықты анықтау құралдарын құру үшін анық емес модельдер жиыны мен әдістерін қолдану басып кірулерді анықтау жүйесін жетілдіруге және қоршаған ортадағы белсенділікті бақылау арқылы қауіпті ауытқушылық жағдайды айқындауға мүмкіндік береді. Осы мақсатта эталонды мәндерді құру үрдісін қалыптастыруға және шабуылдың түрі мен оның атрибуттарын айқындауға қажет сәйкестіктерді табуға мүмкіндік беретін анықталмаған, әлсіз қалыптасқан орта үшін базалық шамалар моделі мен эталонды шамалар моделі құрастырылды. Құрылған шешуші ережелер моделі эталонды шамалар жиыны мен түйіндес жұптар мен айқын емес сәйкестендіргіштер үшін қалыптасқан инициализация матрицасын сарапшылық бағалау әдістері арқылы шешуші ережелер жиынын қалыптастыру үрдісін ауытқушылық жағдайды анықтауға арналған шешуші ережелер жиынын қалыптастыру үрдісін қалыптастыруға мүмкіндік береді. Аталған модельдер мен қалыптасқан ағымдағы шамалардың есебінен сигнатуралық емес және кибершабуылдардың жаңа түрлерін анықтауға арналған құралдарды құруға мүмкіндік беретін ауытқушылық жағдайларды анықтау технологиясы құрылды. Технология негізінде желі жүйесінің қауіпсіздігін жетілдіруге арналған құрылымдық шешім ары қарай дамытылды және шабуылдарды анықтаудың қазіргі заманғы жүйесінің қызметін кеңейткіш ретінде немесе дербес қолданылатын ауытқушылық жағдайды анықтауға арналған алгоритмдік және бағдарламалық қамтамасыздандыру құрылды.

**Тақырыптың өзектілігіне** байланысты сигнатуралық емес желілік кибершабуылдардан туындайтын анық емес жағдайларда ауытқуларды анықтау жүйесінің, әдістері, моделдері және технологиялары негізінде шабуылдарды табу жүйелердің мүмкіндіктерін арттыратын заманауи құралдар әзірлеумен анықталады.

**Зерттеу мақсаты** компьютерлік желілерде сигнатуралық емес кибер шабуылдар түрін анықтау жүйесінің мүмкіндіктерін артыру үшін, ауытқу күйін сәйкестіндіру үшін, моделдер мен құралдарын әзірлеу болып табылады.

Қойылған мақсатқа жету үшін келесі негізгі міндеттерді шешу керек болды:

1. Компьютерлік желілердегі шабуылдарды анықтау үшін қолданылатын теориялық және тәжірибелік базалардың қазіргі заманғы даму жағдайын зерттеу;

2. Компьютерлік желілердегі кибер шабуылдардың белгілі бір, қоршаған ортадағы ауытқу жағдайын өлшемін көрсететін және базалық шамалар моделі мен эталонды шамалар моделін құрастыру;

3. Базалық шамалар моделі мен эталонды шамалар моделінің негізінде қалыптастыру үшін ауытқу жағдайын анықтауға арналған шешуші ережелер моделін құру;

4. Базалық шамалар моделі, эталонды шамалар моделі және шешуші ережелер модельдерінің негізінде тіркелмеген әрекеттерді тудырған ауытқу жағдайын анықтау технологиясын әзірлеу;

5. Ауытқу жағдайын анықтау технологиясы негізінде сигнатуралық емес кибер шабуылдарға бағытталған басып кіру жүйесінің функционалдық мүмкіндіктерін кеңейту үшін құрылымдық шешім шығару;

6. Компьютерлік желілердегі шабуылдаушы әрекеттерді анықтауға мүмкіндік беретін жаңа техникалық шешімдерді әзірлеу және эксперименталды зерттеу жүргізу.

**Зерттеу объектісі–** компьютерлік желілерде шабуыл әрекеттерімен жинақталатын ауытқымалы жай-күйін анықтау процесі;

**Зерттеу пәні** - модельдер, әдістері, тәсілдері және компьютерлік желілерді шабуыл жүйесінің әрекеттері мен жинақталатын ортада нақты емес аутқымалыны табу жүйесі

**Зерттеу нәтижелерінің ғылыми жаңалықтары**

Диссертациялық зерттеуді орындау аясында төмендегідей ғылыми зерттеулер алынды:

1. Белгілі бір желілік шабуылдардың жиынтығына тән, анық емес айнымалы эталондарын құру процесін қалыптастыруға мүмкіндік береді және қоршаған ортадағы ауытқу жағдайын өлшемін көрсету **«шабуыл: түйіндес жұп жиынтығы» және «шабуыл: шамалар»** жұп жиынтығының негізінде ендірілген шамалардың есебінен, базалық шамалардың моделі және эталонды шамалардың моделі ұсынылды; ары қарай дамытылды

2. Компьютерлік желілердегі ауытқу жағдайын сарапшылық жолмен анықтауға арналған шешуші ережелер жиынын қалыптастыру мүмкіндігін береді, эталонды шамалар жиынының есебінен түйіндес жұп пен анық емес сәйкестендіру матрицасын сарапшылық бағалаудың әдістерімен қалыптасқан шешуші ережелер моделі ары қарай дамытылды;

3. Тұңғыш рет шабуылдарды анықтау жүйесі үшін лингвистикалық эталондарды қалыптастыру әдісі құрастырылды, ол нақты гетереогенді параметрлі ортада түрлі ауытқушылық жағдайын сипаттайтын берілген лингвистикалық айнымалылар топтарының шамалардың эталонды мәндерін алу процедурасын қалыптастыруға мүмкіндік береді

4.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 жағдайларды анықтау технологиясы құрылды;

5. Анық емес арифметика модулі және ішкі жүйелердің есебінен ауытқушылық жағдайын анықтау технологиясының көмегімен жүзеге асырылған басып кірулерді анықтау жүйесінің құрылымдық шешімі; желілік шамалардың айқын емес эталондарын қалыптастыру; шешуші ережелерді және алғашқы өңдеуді қалыптастыру қоршаған ортадағы белсенділікті бақылау басып кірулерді анықтаудың қазіргі заманғы жүйесінің функционалды мүмкіндіктері ары қарай дамытылды**.**

**Зерттеу әдістері** анық емес теориясы, жиынтықтар, шешім қабылдау алгоритмдерін, модельдеу, ақпараттық процестер мен құрылымдардың модельдеу, сондай-ақ сараптама және есептеу әдістеріне негізделген.

Кіріспеде зерттеудің өзектелігі, зерттеу мәселесіне байланысты проблемалар нақтыланды. Жұмыстың идеялары, зерттеудің мақсаттары мен міндеттері, жұмыстың ғылыми жаңалықтары мен практикалық бағалығы келтірілген.

**Бірінші бөлімде.** Әдістер және шабуылдарды жүзеге асыру құралдарына сараптама жасалды, олар біршама кең спектрді құрайтыны, үздіксіз жетілдірілетіні компьютерлік жүйелер мен желілердегі тіркелмеген әрекеттерді жүзеге асыруда қолданылады. Нейрожелілік ұстанымдар статистикалық әдісінің қолданылатын бағытты негізінен ШТЖ кең таралған. Статистикалық мәліметтердің жеткіліксіз іріктемесіне, қоршаған ортадағы күтпеген өзгерістерге, жүйені оқытудағы қателіктерге, белгісіз шабуылдарға (мысалы «0-day" және белгілі шабуылдардың түрленуі басып кірулерді анықтауда белгілі қиындықтарға әкеледі) біршама сезімтал болып келеді.

**Екінші бөлімде** ШТЖ ауытқу жағдайын анықтау моделдерін жасауға арналған. “Басып кіру : шамалар” және “басып кіру **:** түйіндес жұптар жиыны ”жұптар жиынын ескере отырып, базалық шамалар модельдері мен эталонды шамалар модельдері негізінде кибершабуылдардың нақты түрі туындатқан ауытқушылық жағдайын көрсетуге мүмкіндік беретін шешуші ережелер моделі ұсынылды.

ШЕМ құру үшін анық емес идентификаторлар жиыны еңгізілді (fuzzyidentifiers).

**Үшінші бөлім**де желілік шабуылдардан пайда болатын ауытқушылықты анықтаудың технологиясын әзірлеуге және ауытқуды табу жүйелеріне арналған жаңа құрылымдық шешімдерге арналған. Ұсынылған технология екінші тарауда әзірленген математикалық модельдер және анық емес логиканың әдістеріне және бірінші бөлімде талданды түйіндемелерге негізделген. Онда сегіз негізгі кезеңдер бар, ол кибершабуылдың нақты түрімен туындаған ауытқулар жағдайын анықтау үдерісін анықтайды.

**Төртінші бөлім** компьютерлік желілердегіауытқушылықтарды анықтау құралдарын зерттеу мен тәжірибелік жүзеге асыруларға арналған. Порттардды сканерлеу туындатқан, ұсынылған ауытқушылықтарды алгоритмдік қамсыздандыру және типтік жүйе негізінде сканерлеуші құралдарды анықтаудың бағдарламалық жүйесіне және шабуылдаушы әрекеттер туындатқан ауытқушылықтарды анықтаудың қолданбалы жүйесіне тәжірибелік зерттеу жүргізілді**.** Сонымен бірге ұсынылған әдісті жүзеге асыратын жүйенің негізігі жұмысы көрсетілген, түрлі кибершабуылдардың үшін алынған түрлі ауытқушылық жағдайлардың графикалық түсіндірмесі берілген,ал негізгі эксперимент Ұлттық авиациялық университеттің ақпараттық технологиялар қауіпсіздігі кафедрасының жұмыс бекеттеріне 1500 басып кірулерді(шабуылдарды) модельдеу жолымен жасалды

Осымен бірге басып кірулерді анықтау 29,3 % жағдайда $SR_{15}$ = “Егер $\underset{\sim}{t}_{VCA}$ $\underset{\sim}{T}^{e}_{VCA}$ енетін $\underset{\sim}{Y}^{e}$ неғұрлым жақын болса және $\underset{\sim}{t}_{NVC}$ $\underset{\sim}{T}^{e}_{NVC}$ енетін $\underset{\sim}{VB}^{e}$ неғұрлым жақын болса, онда *SN* тудырған ауытқушылық жағдайының деңгейі LIM болады”ережесін ал 38,7 % және 32 % сәйкесінше $SR_{14}$ және $SR_{13}$ ережелерін бастамашылыққа алатынын атап өткен жөн.

Жүргізілген верификация нәтижелерінен барлық басып кірулер сарапшының түрлі сенім дәрежесін көрсететін түрлі ережелер арқылы анықталғаны көрінеді. Осыған сәйкес ұсынылған моделдер мен жүйелерді жүзеге асыру үлгіленетін әрекеттерге реакция бейнелейтіні туралы қорытынды жасауға болады.

**Қорытындыда** диссертациялық жұмыстың негізгі нәтижелері және қорытындылары көрсетілген.

**Жұмыстың практикалық маңыздылығы.**

Диссертациялық жұмыста алынған нәтижелер ауытқушылықтарды анықтау үшін программалық-аппаратты модульдер немесе программалық модульдер түрінде техникалық

шешімдер құрғанда және автономды немесе қазіргі заманғы ШАЖ функционалдығын кеңейткіш ретінде қолданылуы мүмкін. Практикалық маңыздылығы келесіде:

- құрылған модельдер және технлогия негізінде 1701 «Ақпараттық қауіпсіздік» саласында мамандарын дайындайтын оқу барысында қолданылатын лабораториялық жұмыс және дәрістік материал құрылды. Диссертациялық зерттеудің практикалық қолданылуы Ұлттық авиациялық университет (Киев, Украина) оқу процесіне еңгізу актімен (17.02.2017ж) расталады.
- ауытқу күйді анықтаудың ұсынылған технологиясы негізінде айқын емес нақты қалыптасқан ортада ақпараттық жүйелер ресурстарына кибершабуылдарды анықтауға мүмкіндік беретін «Айқын емес логика негізінде порттарды сканирлеуді анықтау» компьютерлік программасы құрылды, ол ақпараттық жүйе қорғалу дәрежесін жақсарту және қорғау желілік жүйесінің жұмыс тиімділігін оңтайландыруға мүмкіндік берді, ол «Сайфер БІС» ЖАҚ жұмысына еңгізу актімен расталады (03.02.2017).

**Зерттеу нәтижелерінің аппробациясы**

Зертеудің негізгі нәтижелері төмендегі конференцияларда баяндалды:

- Ақпараттық және телекоммуникациялық технологиялар: білім, ғылым, тәжірибе» атты **II Халықаралық ғылыми-тәжірибелік конференция еңбектер**. Қ.И Сатпаев атындағы ҚАЗҰТУ Алматы. Шабуылдарды табу жүйесіне арналған бағалау сараптамасының әдісін талдау
- «Қазіргі ақпараттық және телекоммуникациялық технологиялар»: **Халықаралық ғылыми-тәжірибелік конференция Украина, Киев 2015 ж** Шабуылдарды табу жүйелерін құру үшін анық емес жинақтар әдістерін талдау.
- Басқару және автоматтандыру жүйелер бойынша 16-шы халықаралық конференция / **ICCAS.2016 Gyeongju, Оңтүстік Корея, 2016** Шаблонды және өлшеу шабуылдары мен ақпарат құнының критериясы бойынша желілік модельді бағалау**.**
- «Ақпараттық және телекоммуникациялық жүйелердің қауіпсіздігі мен жағдайы» **(SITS-2016). //-Николаев-Коблева:** Халықаралық технологиялық университеті Кибер қауіпсіздік ақпараттық-психологиялық аспектілері
- **ITSEC - VI Халықаралық** ғылыми-техникалық конференциясы 2016. Украина, Киев Ұлттық авиациялық университеті. Ақпараттық ресурстардағы шабуылдардың параметрлерін анықтау үшін ақпараттық-аналитикалық жүйе
- Киберқауіпсіздікті және ақпаратты қорғауды қамтамасыз етудің өзекті мәселелері: **II Халықаралық ғылыми-практикалық конференция (Украина, Киев 2016)** Кибершабуылды анықтау жүйелеріне арналған шартты анықтау анықтамаларын құру әдістемесі
- Киберқауіпсіздіктің өзекті мәселелері және ақпараттық қауіпсіздік: **III Халықаралық ғылыми-тәжірибелік конференция:(**Украина, Киев Еуропалық университет, 2017 ж) Сниффинг шабуылдарды анықтау үшін лингвистикалық стандарттарды құру

Басылымдар. Берілген ғылыми зерттеу 23 жұмыс жарияланған, оның 8 -ҚР БҒМ - Білім және ғылым саласындағы бақылау комитеті ұсынған басылымдарда жариаланған, 4 мақала Scopus мәліметтер қорына кіретін баылымдар жарияланған, 4 мақала ғылыми журналдарда және ғылыми еңбектер жинақтарында жарияланды: халықаралық конференциялар жинағында (Украина) 5 мақала, халықаралық конференцияның материалдарында 2 мақала жарияланды (Қазақстан).

**Диссертация құрылымы мен көлемі**. Диссертация кіріспеден, төрт бөлімнен, жалпы қортындылардан, қосымшалардан, қолданылған әдебиеттер тізімнен тұрады және негізгі мәтін 165 парақты, 41 сурет, 23 кесте, әдебиеттер тізімі 113 атаудан тұрады. Жұмыстың жалпы беттер саны 185 бет.

Диссертация тақырыбы бойынша 23 мақала жарияланды:


1. Ахметов Б.С. Использование методов нечетких множеств в системах обнаружения вторжений / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева // Інформаційна безпека. – 2014. – №1 (13); №2 (14). – С. 42-55.

2. Использование методов експертного оценивания в системах обнаружения вторжений/ Б.С. Ахметов, А.А. Корченко, С.Т. Ахметова, Н.К. Жумангалиева // Інформаційна безпека. – 2014. – №3 (15); №4 (16). – С. 34-43.

3. Ахметов Б.С. Анализ методов нечетких множеств для построения систем обнаружения вторжений /Б.С.Ахметов, А.А.Корченко, Н.К.Жумангалиева //«Современные информационно-телекоммуникационные технологии»: Междунар. науч.-тех. конф. : Матер. конф. – К.: ГУТ, 17-20 ноября 2015 года – С. 38-40.

4. Базовые модели эталонных величин для систем обнаружения вторжений / Б.С. Ахметов, Р.Б.Абдрахманов, А.А.Корченко, Н.К. Жумангалиева // ВестникМеждународногоКазахско-Турецкогоуниверситета. им. А.Ясави. – 2015. – №5-6 (97-98). – С. 15-26

5. Анализ методов экспертного оценивания для систем обнаружения вторжения / Б.С. Ахметов, А.А. Корченко, С.Т. Ахметова, Н.К. Жумангалиева // «Информационные и телекоммуникационные технологии: образование, наука, практика» : II междунар. науч.-практич. конф. : Труды. – Алматы, Казахстан, 3-4 декабря, II том. – 2015 года. – С. 28-31.

6. Ахметов Б.С. Модель базовых величин для контроля аномальности состояния среды окружения / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева// Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая. – 2016. – №1 (305). – С. 26-33.

7. Ахметов Б.С. Модель решающих правил для обнаружения аномалий в информационных системах / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева // Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая. – 2016. – №4 (308). – С. 91-100.

8. Метод построения условных детекционных выражений для систем обнаружения кибератак / Н.П. Карпинский, А.А. Корченко, С.Т. Ахметова, Н.К. Жумангалиева // Актуальні питання забезпечення кібербезпеки та захисту інформації : II міжнар. наук.-практ. конф. : Тези доп. – Київ, 24-27 лютого 2016 року – С. 65-69.

9. Ахметов Б.С. Технология выявления аномального состояния для систем обнаружения вторжений / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева // Вестник КазНУ. Серия математика, механика, информатика. – 2016. – №1 (88). – С. 106-113

10. Akhemtov Bakhytzhan, Korchenko Anna, Akhmetova Sanzira, Zhumangalieva Nazym. Improved method for the formation of linguistic standards for ofintrusion detection systems // Journal of The oreticaland Applied Information Technology, 2016. Vol.87. №.2. – Pp. 221-232.

11. Корченко А.А. Построение лингвистических эталонов для выявления сниффинг атак / А.А. Корченко, Н.К. Жумангалиева, П.А. Викулов // Актуальні питання забезпечення кібербезпеки та захисту інформації : III міжнар. наук.-практ. конф. : Тези доп. – Київ, 22-25 лютого 2017 року – С. 93-97.

12. Ахметов Б.,Иванов А., Алибиева Ж., Мукапил К., Бекетова Г. Prospects for Multiple Reductions in Test Samples with a Multivariate, Multicriteria, The Neural Network Statistical

Analysis of Biometric Data // Medwell Journals, 2015 Research Journal Applied Scienses 10(12) 2015 956-967

13. Mikolaj Karpinski, Vasyl Martsenyuk, Iryna Gvozdetska, Bakhytzhan Akhmetov, Zhumangalieva Nazym. Estimation Problem for Network Model at State and Measurements Attacks and Information Cost Criterion// 16th International Conference on Control, Automation and Systems / ICCAS.2016.7832298 Gyeongju, South Korea, 2016, pp. 45-50.doi: 10.1109/

14.Aleksandra Kłos-Witkowska; Bakhytzhan Akhmetov; Volodymyr Karpinskyi; Tomasz Gancarczyk. Bovine Serum Albumin stability in the context of biosensors//2016 16th International Conference on Control, Automation and Systems (ICCAS)//Year:016//Pages: 976 80, DOI: 10.1109/ICCAS.2016.7832427EEE Conference Publications

15. Ахметов Б.С., Корченко А.А. Смагулов С.К , Жумангалиева Н:К . Ақпараттық жүйенің жағдайын бақылауға арналған базалық ауытқымалық шаманың модельдері// Семей Қаласының Шәкәрім Атындағы Мемлекеттік Университетінің х а б а р ш ы с ы 2016 № 2 (74) -С . 87 -91

16. Ахметов Б.С., Корченко А.А. Смагулов С.К , Жумангалиева Н.К . Ақпараттық жүйенің аномалиялық жағдайын бақылауға арналған базалық шаманың модельдері// Семей Қаласының Шәкәрім Атындағы Мемлекеттік Университетінің х а б а р ш ы с ы № 1 (77) 2017 С 111-115 ISSN 1607-2774

17. B. Akhmetov, A. Korchenko, J. Kultan, N.Zhumangalieva,. Model decision rules to detect anomalies in Information Systems// Informational Technology Application, Словакия, №1, 2016 126-136 ISSN 13386468

18. Бекетова Г. С., Ахметов Б.С., Абишева Г.К., Жумангалиева Н.К . Жеке биометриялық мәліметтерді қорғаудың нейрожелілік технологиясы//«Қазақстанның жаңа экономикалық саясатын таратуда жас ғалымдардың орны мен рөлі» халықаралық Сәтбаев оқуларының еңбектері, IV том, 2015 ж., с- 719-724

19. Мукапил., Бекетова Г. С., Төлімесова В., Жумангалиева Н.К . Ақпаратты қорғаудың биометриялық әдістері// Хабарщысы КазҰТУ. №2, 2015 г. с.250-261.

20. Мукапил., Бекетова Г. С., Төлімесова В., Жумангалиева Н.К ., Култан Я.. Biometric methods of nformational protection// Informational Technology Application, Словакия, №1, 2016 126-136

21. Ахметов Б.., Алимсеитова Ж., Коренко А., Жумангалиева Н.К . Система выявления аномального состояния в информационных системах// Қазақстан Республикасы Ұлттық ғылым академиясының баяндамалары Физика -математика 2017. – №5 (308). – С. 28-37

22. Ахметов Б.., Коренко А., Жумангалиева Н.К., Култан Я.. Model decision rules to detect anomalies in Information Systems// Informational Technology Application, Словакия, №1, 2016 126-136

23. Гнатюк С.О., Шаховал О.А., Бекетова Г., Жумангалиева Н.К.. Информационно-психологический аспект киберзащиты// «Состояние и совершенствование безопасности информационно-телекоммуникационных систем» (SITS-2016). //– Николаев-Коблево: Международный технологический университет, 9-12 июнь 2016 г. 32-34