

6D070400 – «Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы бойыншы PhD докторанты М.Н. Жекамбаеваның «Ақпараттық ресурстардың қауіпсіздік қатерін бағалау мен анализдеу әдістері» тақырыбындағы диссертациялық жұмысына

## АНДАТПА

**Зерттеу тақырыбының өзектілігі.** Кәсіпорынның ІТ-инфрақұрылымының қарқынды дамуы ақпараттық ресурстардың (АР) әлсіздігі мен қауіп-қатер санының өсуін бақылай алмайтындыққа алып келеді. Мұндай жағдайда, қатерлерді басқару жүйесін және ақпараттық қауіпсіздікті қамтамасыз ету бойынша жұмыстардың жоспарын жасаған кезде қатерді бағалау мен анализдеу қажетті шарттылық болып табылады.

Қазіргі кезде, бағалау үшін қолданылатын, айтарлықтай кең спектрде берілген яғни нормативті құжаттардан (стандарттардан) басталып, нақты программалық қосымшалармен аяқталатын қатерді бағалау мен анализдеудің көптеген құралдары (ҚБАҚ) бар. Практикалық қызметте қолдану үшін соңғыларын таңдау кезінде сарапшы көптеген сұрақтармен соқтығысады, мәселен, мынадай, «Қандай параметрлерді қолданған жөн?», «Қанадай математикалық аппарат қолданылады?», «Статистикалық мәліметтерсіз қалай бағалауға болады?», «Анық емес шарттылығында қатерді бағалау мен анализдеуді қалай жүзеге асыруға болады?» т.б. Осы және өзге факторлар сәйкес келетін бағалау амалын таңдау кезінде бірқатар қиындықтар туғызады.

Сонымен бірге, айта кететін жайттардың бірі, негізінде ақпараттық қауіпсіздік қауіп-қатерлері мен оқиғалары туралы статистикалық мәліметтер қатерді бағалау мен анализдеу үшін қолданылады. Көптеген елдерде соның ішінде Қазақстан да осындай статистиканы тіркеу мен қолдануға қатысты мемлекеттік айла-құралдар жоқ, бұл өз кезегінде мемлекетте қолдану үшін бар болған құралдардың мүмкіндігін шектейді. Сарапшының қатерді бағалау кезінде параметрдің кеңдеу спектрін қолдану мүмкіндігін қиындататын және бір фактор – бұл осындай құралдарда белгілі бір шектеулердің (қолданылып жатқан параметрлер жиынына) бар екендігі болып табылады, бұл өз кезегінде олардың икемділігін төмендетеді.

Сондықтан, ҚБАҚ және әдістерді зерттеу мен өңдеу ақпараттық қауіпсіздік қатерін бағалау мен анализдеу аспаптарын қолдану кезінде айтарлықтай икемді жасауға мүмкіндік беріп, статистикалық мәліметтер, сонымен қатар, анық емес, әлсіз қалыптасқан ортада жасалған сарапшылық бағалаулар негізінде сәйкес келетін тапсырмаларды тиімді шешуі **зерттеу тақырыбының өзектілігі мен оның мақсаты болып табылады.**

### **Зерттеудің негізгі міндеттері:**

1. Ақпараттық қорғаудың тапсырмаларын шешуде тиімдірек аспапты жасау мен таңдау үшін қолданылатын сипаттама қорының жинағын анықтау мақсатында қатермен байланысты негізгі түсініктерді, бар болған стандарттарды,

әдістерді, әдістемелерді, әдіснамаларды және программалық ҚБАҚ-ды зерттеу мен талдау;

2. Алынған сипаттама қоры негізінде көлемнің жиынтығын динамикалық анықтауға мүмкіндік беретін қордың қортежді моделін (ҚКМ) өңдеу және осылай сәйкесінше ақпараттық қауіпсіздік ҚБАҚ өңдеуде икемділікті қамтамасыздандыру;

3. Қордың қортежді моделі (ҚКМ) есебінен бағалаудың тиімді құралдарын жасауға мүмкіндік беретін, анық емес анықталған сипаттама қоры мен детерменттелген жиынтығын динамикалық түрде өзгертетін кіріс мәліметтер түрінде қолданылушы ақпараттық қауіпсіздік қатерін бағалау мен анализдеу әдісін өңдеу;

4. Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу тапсырмаларын шешу кезінде  $n$ -еселі инкременттелген эталонды параметриялық трапеция түріндегі анық емес сандарға (АЕС) негізделетін лингвистикалық айнымалы (ЛА) тәртібін (термдер санын) эквивалентті түрде алдын ала анықтауға мүмкіндік беретін әдістерді өңдеу. Бұл көрсетілген жүйелердің әрі қарай дамуына септігін тигізеді және олардың трапециялық түрегі және үшбұрышты анық емес сандарын қолдану құралдары бойынша мүмкіндіктерін кеңейтеді;

5. Ұсынылған әдістер мен модельдер қолданылған, қатерді тиімді бағалауға арналған программалық сияқты программалық-аппаратты жүйесінің құрылым процесін нысандандыру мен жинақтап қорытуға мүмкіндік беретін, ақпараттық қауіпсіздік қатерін бағалау мен анализдеу жүйесін синтездеу әдіснамасын өңдеу;

6. Ақпараттық қатерлер саласындағы мәселелерді шешу үшін ұсынылған әдістерді, модельдері және әдіснамаларды қолданатын жүйелердің жаңа құрылымдық шешімін өңдеу;

7. Бар болған жүйелердің ұсынылған әдіснамасы мен құрылымдық сұлбасы негізінде өңделген әдістерді, моделі мен құрылымдық шешімдерін тексеру мақсатында программалық ҚБАҚ қамтамасыздандыруын программалық қамтамасыздандыру (ПҚ) экспериментальді зерттеуді жүзеге асыру мен өңдеу;

**Зерттеу объектісі** – Ақпараттық қауіпсіздік қатерді бағалау мен анализдеу процесі.

**Зерттеудің пәндік аймағы** – Ақпараттық қауіпсіздік саласындағы қатарді бағалау мен анализдеу құралдарының программалық құралдары, әдістері, жүйелері, модельдері және әдістемелері.

**Зерттеу әдістері.** Жүргізілген зерттеулер анық емес логика теориясының заманауи әдістеріне (қатерді бағалау мен анализдеу әдістерін өңдеу, сонымен бірге лингвистикалық айнымалының терм санын  $n$ -еселі инкременттеу әдісін өңдеу), алгоритмдер шешімін қабылдауға, бағытталған-объектті программалау (ақпараттық қауіпсіздік, ҚБАҚ, ПҚ өңдеу), ақпараттық процесстер мен құрылымын еліктеп моделдеуге (экспериментальді зерттеуді жүргізу кезінде

ақпараттық жүйе жай-күйінің ортасы мен әр түрлі шарттылықтарын модельдеу), сонымен бірге жайлы есептеуге негізделеді.

**Зерттеудің ғылыми жаңалықтары** келесіде өз шешімін табады:

- алты компоненттік кортежбен бейнеленген сипаттама қорын талдап қорыту есебінен талап етілетін сипаттамалар жинағының жиынтығын қалыптастыру мүмкіндігін есепке алатын қатерді бағалау мен анализдеудің тиімді, әрі икемдірек әдістерін жасауға мүмкіндік беретін *алғаш рет* қатердің сипаттама қорының кортежді моделі өңделді;

- *мұнан былайғы дамуды алдық* қатерді бағалау мен анализдеу әдістері детерменттелген және анық емес анықталған параметрлер қоры жинағының динамикалық түрде өзгеруін өңдеудегі логикалық-лингвистикалық айнымалы және қатердің сипаттама қорының кортежді моделі есебінен бағалаудың интеграцияланған мүмкіндігі бар тиімді амалын жасауға мүмкіндік береді;

- бірінші және екінші жеке қор кеңейуін қолданумен  $n$ -еселі инкременттелген терм сандарының функциясын жүзеге асыру әдісін *алғаш рет* өңдеу; мұнда термдерді бір тәртіпке инкременттеу функциясын  $n$ -еселі кеңейту модификациясының есебінен сарапшыларды сәйкесінше құрал-жарақ саласына жұмылдырусыз  $n$  тәртіптерге лингвистикалық айнымалы термдерінің эталонды санын эквивалентті трансформаторлау процесін қалыптастыру мүмкіндігі кеңейеді;

- Ақпараттық қауіпсіздік қатерін бағалау мен анализдеу кезінде өңделіп жатқан көлемінің берілген жиынтығын қолданудың икемденгіш мүмкіндігі бар аспаптық құралдарды жасау процесін қалыптастыруға мүмкіндік туғызатын ақпараттық қауіпсіздік қатерін бағалау мен анализдеу жүйесін синтездеу *мұнан былайғы дамуды алдым* әдіснамасы;

- *мұнан былайғы дамуды алдық* ақпараттық қауіпсіздік қатерін бағалау мен анализдеу жүйесінің құрылымдық шешімі ұсынылған әдістерін жүзеге асырушы мәліметтерді қалыптастыру мен сипаттама қорының өңделген ішкі жүйесі есебінен мәліметтерді сапалық, әрі сандық интерпретациялау түрінде қайта жаңғырту мен қалыптастыруға мүмкіндік береді;

**Жұмыстың практикалық құндылығы** мыналарда өз көрінісін тапқан:

- ұсынылған синтездің өңдеу әдіснамасының және жүйелердің құрылымдық шешімі негізінде ақпараттық қауіпсіздік программалық ҚБАҚ-н жүзеге асуы үшін алгоритм түзілген ;

- ҚБАҚ құру кезінде қолданылуға болатын бұзылған ақпараттық қауіпсіздіктің қауіп-қатері мен оқиғасының, АР-дың біріктірілген мәліметтер қоры өңделген;

- ұсынылған алгоритм мен біріктірілген мәліметтер қоры негізінде сипаттама қорының әр түрлі жинағын динамикалық түрде анықтайтын және қолданатын, детерминдендірілгенде де, анық емес, әлсіз құрастырылған ортада да икемдігін, функционалдығын және оны қолдануда ыңғайлылығын көтеретін, ақпараттық қауіпсіздік ҚБАҚ-дің қолданбалы программасы жүзеге асырылады

Зерттеу нәтижелері Қ.И.Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университетінің «Ақпараттық қауіпсіздік» кафедрасының оқу процессінде қолданылды, Ұлттық авиациялық университетінде (Киев, Украина) «Ақпараттық технологиялар қауіпсіздігі» кафедрасы сонымен қатар «Ақпараттық технологиялар қауіпсіздігі» «ДЕЛЬТА» ООО (Киев, Украина) және ЖШС «QUARES» (Алматы).

**Диссертацияның апробациялық шешімдері.** Диссертациялық жұмыстың негізгі тәртіптері мен нәтижелері ғылыми-техникалық конференциясында, семинарларда, баяндалды және талқыланды сонымен бірге;

– Қ.И.Сәтбаев атындағы ҚазҰТЗУ-дың «Ақпараттық қауіпсіздік» кафедрасында «Ақпаратты қорғаудың қазіргі заманғы технологиялары» ғылыми семинарда;

– Ұлттық авиациялық университетінің (Киев, Украина) «Ақпараттық технологиялар қауіпсіздік» кафедрасының ғылыми семинарында;

– Қ. И. Сәтбаев атындағы ҚазҰТУ-ң 80 жылдығына арналған «Қазақстан-2050» Стратегиясының іске асырудағы жас ғалымдардың орны мен рөлі» атты Халықаралық Сәтбаев оқулары Алматы, 2014ж.;

– «Ақпараттық және телекоммуникациялық технологиялар» Білім, ғылым, тәжірибе атты II Халықаралық ғылыми-тәжірибелік конференциясы Алматы, 2015ж;

– Қ. И. Сәтбаев атындағы ҚазҰТУ-ң 80 жылдығына орай «XXI ғасырдағы инженерлік білім және ғылым: проблемалары мен келешегі» атты халықаралық форумы, Алматы, 2014;

– Л.Н.Гумилев атындағы Еуразия ұлттық университеті «Қазақстан-2050» Стратегия аясында «Ақпараттық қауіпсіздік» III Халықаралық ғылыми-практикалық конференция, Астана, 2015;

– XV Халықаралық ғылыми-тәжірибелік конференция «Білім берудегі информатика мәселелері, басқару, экономика және технологиялар», Пенза, 2015.

– Second International Scientific-Practical Conferenc «Problems of Infocommunications. Scienceand Technology», Kharkiv, 2015;

– II международная научно-практическая конференция «Актуальні питання забезпечення кібернетичної безпеки та захист інформації», Киев, Европейский университет, 2016.

– Халықаралық ғылыми-тәжірбиелік конференция «Макроэкономикалық талдау және экономикалық саясат жөніндегі математикалық тәсілдер және ақпараттық технологиялар» (академик А. Әшімов 80 жылдығына орай), Алматы, 2017ж.

Диссертациялық жұмыс Қ.И. Сәтбаев атындағы ҚазҰТУ ғылыми-зерттеу жобасының аясында жүзеге асырылды №757.МОН.ГФ.15.ИИТ.6 «Ақпараттық қауіпсіздік Биометрикалық стандарттар қолдау жөніндегі ғылыми-зерттеу, үйлестіру, өзгерту және тіркеу» және Ұлттық авиация университетінің Украина «Ақпараттық жүйелердің қауіпсіздік қатерін бағалау әдістемесі» ғылыми-зерттеу жұмысы (тіркеу №14.01.05 нөмірі 105).

**Мақалалар.** Диссертациялық жұмыстың тақырыбы бойынша 16 ғылыми жұмыс жарияланды оның ішінде; 5 мақала ҚР БЖҒМ Білім саласындағы бақылау комитеті ұсынған журналдарда жарияланғанды, 1 мақала Дерекқор Scopus деректер базасына (Elsevier) индекстелген журналында жарияланды; 10 мақала Халықаралық конференцияларда, оның ішінде 5 шет елдегі конференция, 1 тезис жарияланды.

**Ізденушінің жеке қосқан үлесі.** Автордың өзбетімен алған диссертациялық жұмысының қорғауға енгізетін негізгі тәртіптері мен нәтижелері. Авторласпен бірлікте жазылған жұмыста жеке автордың үлесі төмендегідей: [20, 58, 59, 63] – қатер түсінігінің анализі жүргізілді және ҚКМ моделі өңделді; [77, 78] – ұсынылған модельді қолдану арқылы қатерді бағалау мен анализдеу құралдарын зерттеу жүргізілді; [79] – ақпараттық қауіпсіздік қатерлерін бағалау мен анализдеудің екі әдісі ұсынылды; [80, 81] – ЛА термдер санының n-еселі инкременттелген әдісінің екі нұсқасы берілді; [82-84] – First-ҚБАҚ мен Second-ҚБАҚ жүйелерінің құрылымдық шешімдері мен ақпараттық қауіпсіздік қатерді бағалау мен анализдеудің синтезді жүйесінің әдіснамасы өңделген; [85] – ұсынылған әдіснамалар мен құрылымдық шешімдер негізінде программалық ҚБАҚ өңделді, сонымен бірге, осы жүйелердің экспериментальді зерттелуі жүргізілді. Диссертациялық жұмыста, авторлас жарияланған жұмыстардан, жеке ізденуші алған шешімдер қолданылды.

**Диссертацияның құрылымы мен көлемі.** Диссертациялық жұмыс, кіріспеден, төрт бөлімнен, қорытындыдан, 85 қолданылған әдебиеттер тізімінен тұрады; барлығы 146 бетте көрсетілген, 43 сызбадан, 57 кестелер мен Қосымшадан тұрады.