

Әл-Фараби атындағы Қазақ ұлттық университетінің қарамағында құрылған «6D07300, 8D06101 – Ақпараттық жүйелер», «6D070400 - Есептеу техникасы және бағдарламалық қамтамасыз ету (Компьютерлік инженерия)», «6D075100 - Информатика, есептеу техникасы және басқару (Жүйелік инженерия)», «6D060200 - Информатика (Компьютерлік ғылымдар)», «6D100200, 8D06301 - Ақпараттық қауіпсіздік жүйелері», «6D070200 - Автоматтандыру және басқару» мамандықтар тобы бойынша философия докторы (PhD) дәрежесін беру жөніндегі

### **«Информатика және ақпараттық жүйелер» диссертациялық кеңесінің 2021 жылғы жұмысы туралы ЕСЕБІ**

Диссертациялық кеңестің төрағасы физика-математика ғылымдарының докторы, профессор, ҰҒА академигі Қалимолдаев Мақсат Нұрәділұлы.

Диссертациялық кеңес Ғылыми кеңесінің шешімі негізінде (2021 жылғы 22 маусымдағы №11 хаттама) әл-Фараби атындағы ҚазҰУ Басқарма Төрағасы – Ректордың 28 маусымдағы 2021 жылғы № 306 бұйрығымен бекітілген.

**1. Өткізілген отырыстар саны туралы деректер.** 2021 жылы диссертациялық кеңестің 2 отырысы өткізілді.

**2. Отырыстың жартысынан азына қатысқан диссертациялық кеңес мүшелерінің тегі, аты, әкесінің аты (бар болса).**

Диссертациялық кеңестің барлық мүшелері – 12 адам, олардың ішінде 6 адам (50%) диссертациялық кеңестің тұрақты мүшелері және 6 адам (50%) докторлық зерттеу тақырыбына байланысты докторанттың қорғау кезеңіне уақытша тағайындалды. Өткізілген отырыстың жартысынан азына қатысқан кеңес мүшелері жоқ.

### **3. Оқу орны көрсетілген докторанттар тізімі**

№	Докторанттардың ТАӘ	Ғылыми жетекшілері	Докторант оқыған, ЖОО
1	Алтыбай Аршын	<u>Токмағамбетов Нияз Есенжолұлы</u> – PhD, доцент м.а., әл-Фараби атындағы ҚазҰУ (Алматы қ., Қазақстан);  <u>Michael Ruzhansky</u> – PhD, профессор, Гент университеті (Гент, Бельгия).	Әл-Фараби атындағы Қазақ ұлттық университеті
2	Алғазы Күнболат Тілеуханұлы	<u>Бияшев Рүстем Гакашевич</u> – техника ғылымдарының докторы, профессор, ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институты (Алматы қ., Қазақстан);	Әл-Фараби атындағы Қазақ ұлттық университеті

		Анджей Смолартс – техника ғылымдарының докторы, профессор, Люблин техникалық университеті (Люблин қ., Польша).	
--	--	--	--

#### **4. Мынадай бөлімдері белгіленіп көрсетілген, есепті жыл ағымында кеңесте қаралған диссертацияларға қысқаша талдау**

**Алтыбай Аршын.** Диссертация тақырыбы: «Development of high-performance parallel algorithms and software complex for modeling hyperbolic type equations with singular coefficients: tsunami and acoustic wave propagation».

##### **1) Қаралған жұмыстар тақырыптарына талдау.**

Зерттеу тақырыбының өзектілігі. Қазіргі кезде кездейсоқ пайда болатын және тез өзгеретін физикалық құбылыстар орасан зор экологиялық және экономикалық проблемаларға алып келедуде. Сондықтан мұндай процестерді модельдеу өте өзекті мәселе болып табылады. Осындай есептердің көпшілігі сингулярлы коэффициенттері бар гиперболалық типтік теңдеулермен модельденеді.

Шварццтың дистрибутивті, сингулярлы коэффициентті теңдеулердің классикалық шешімінің жоқ екендігі туралы әйгілі еңбегінен кейін осындай есептерді шешу ашық проблема болып табылады, көптеген зерттеушілер мұндай есептерді шешудің әртүрлі жолдарын ұсынуда, бұл жұмыста сондай әлістердің бірі өте әлсіз шешімдер тұжырымдамасы қолданылады. Яғни бұл жұмыста сингулярлы коэффициентті цунами теңдеуінің өте әлсіз шешімі бар екені және оның жалғыздығы, дәйектілігі туралы теориялық зерттеуде қарастырылған.

Жоғарыдағыдай тез өзгеретін физикалық құбылыстарды ұзақ уақыт және үлкен аумақта модельдеу үлкен есептеу ресурстарын және көп уақытты қажет етеді, егер есептеу алгоритмі тізбекті болса онда ол өте көп уақыт алуы мүмкін мұндай жағдайда параллельді есептеудің маңыздылығы артады.

Көптеген инженерлік және ғылыми қосымшалар көбіне айнымалы коэффициентті теңдеулердің көп мөлшерін параллельді шешуді қажет етеді. Бұл диссертациялық жұмыстың басты мақсаты - әр түрлі заманауи параллельді процессорлық архитектуралардың есептеу қуатын жаңа алгоритмдер мен шешімдерді ұсыну арқылы кейбір математикалық есептердің есептеу жылдамдығын арттыру үшін пайдалану.

Ғылыми жаңалық. Цунами теңдеуінің өте әлсіз шешімдерінің бар екендігін, бірегейлігі мен дәйектілігін дәлелдеу және сандық модельдеу арқылы негіздеу. Сингулярлы коэффициентті екі өлшемді толқын теңдеудің сандық шешудің параллель алгоритмін, айқын емес айырымдылық схемасы негізінде MPI технологиясын қолдану арқылы әзірлеу. Екі өлшемді цунами теңдеуін сандық шешудің параллель алгоритмін айқын емес айырымдылық схемасы негізінде CUDA технологиясын қолдану арқылы әзірлеу. Акустикалық екі өлшемді толқын теңдеуін сандық шешудің параллель гибридік алгоритмін айқын емес айырымдылық схемасы негізінде әзірлеу.



Сингулярлы коэффициенттері бар гиперболалық теңдеуді сандық шешуге және зерттеуге арналған кросс-платформалық ашық кодты программалық қамтама әзірлеу.

**2) Диссертация тақырыбының «Ғылым туралы» Заңының 18-бабының 3-тармағына сәйкес Қазақстан Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия қалыптастыратын ғылымның даму бағыттарына және (немесе) мемлекеттік бағдарламалармен байланысы.**

Диссертациялық жұмыс № АР08052028 «Бессель типті операторлармен және оның қосымшаларымен байланысты стандартты емес гармоникалық талдау» жобасы аясында орындалған.

**3) Диссертациялар нәтижелерінің практикалық қызметке ену деңгейін талдау.**

Жұмыстың практикалық маңыздылығы. Сингулярлы коэффициентті гиперболалық теңдеулерді сандық шешу үшін әзірленген параллель алгоритмдер, Каспий теңізіндегі цунамиді модельдеу үшін қолданылады. Әзірленген программалық қамтаманы ғылымның әр түрлі салаларында біртекті емес ортадағы толқындарды сандық модельдеуге, зерттеуге қолдануға болады.

**Алғазы Күнболат Тілеуханұлы.** Диссертация тақырыбы: «Әртүрлі әдістерге негізделген шифрлау алгоритмдерін құру және зерттеу».

**1) Қаралған жұмыстар тақырыптарына талдау.**

Зерттеу тақырыбының өзектілігі ақпараттық қауіпсіздікті қамтамасыз ету мақсатында ақпараттық-коммуникациялық технологиялардың қарқынды дамуы мен ақпараттық қауіпсіздіктің қолданыстағы түрлерін жетілдіру қажеттілігіне байланысты. Ақпаратты өңдеу, сақтау, беру және пайдалану үдерістері заманауи қоғам өмірінің басым бағытына айналды және көбінесе байланыс құралдары мен ақпарат беру тәсілдерінің дамуы мен қолданылу деңгейіне тәуелді. Қазіргі жағдайда ақпараттың қорғалуы тек мемлекеттік сектор тарапынан ғана емес, сондай-ақ қарапайым тұтынушылар мен үкіметтік емес ұйымдардың қажеттілігі болып табылады. Ақпаратты қорғаудың заманауи құралдарын құру арқылы оны қорғаудың қажетті деңгейін қамтамасыз ету, ақпараттың қауіпсіздігін қамтамасыз етудің өзекті мәселелерінің бірі.

Тәуелсіз мемлекет үшін де ақпараттық және коммуникациялық технологиялар дамуында үлкен рөл атқарады. Қазақстанда 2017 жылы Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») қабылданды. Тұжырымдаманың мақсаты – жаһандық бәсекелестік жағдайда Қазақстан Республикасының орнықты дамуын қамтамасыз ету үшін, электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымдарды сыртқы және ішкі қатерлерден қорғау деңгейіне қол жеткізу және ұстап тұру болып табылады. Осыған

байланысты халықаралық ақпаратты қорғауға қойылатын заманауи талаптарды қанағаттандыратын отандық ақпаратты қорғау жүйелерін құру өзекті болып табылады. Қазақстанда электрондық ақпаратты қорғау үшін негізінен шетелдік криптографиялық құралдар және бағдарламалық жасақтамалар қолданылады, сондықтан отандық криптографиялық қорғау құралдарын құру сөзсіз өзекті және қажет.

Ғылыми жаңалық. Шифрлау алгоритмдеріне қойылатын жалпы талаптарға жауап беретін, ауыстыру-алмастыру жүйесі құрылымындағы жаңа симметриялы блоктық шифрлау алгоритмі құрылды. Дәстүрлі емес әдіске (ПЕПСЖ) негізделген симметриялы блоктық шифрлау алгоритмі құрылды, оны қолдану алгоритмінің криптографиялық беріктігін арттыруға мүмкіндік береді. Дифференциалдық және сызықтық криптоталдауларға беріктілік көрсеткіштері жоғары, сызықты емес (S-блок) ауыстыру түйіндері құрылды.

**2) Диссертация тақырыбының «Ғылым туралы» Заңының 18-бабының 3-тармағына сәйкес Қазақстан Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия қалыптастыратын ғылымның даму бағыттарына және (немесе) мемлекеттік бағдарламалармен байланысы.**

Диссертациялық жұмыс № BR05236757 «Жалпы мақсаттағы желілер мен инфокоммуникациялық жүйелерде ақпаратты жіберу және сақтау кезінде оны криптографиялық қорғау үшін бағдарламалық және бағдарламалық-аппараттық кешендерді құрастыру» бағдарламалық-нысаналы қаржыландыру жобасының ғылыми-зерттеу жұмыстарының аясында орындалған.

**3) Диссертациялар нәтижелерінің практикалық қызметке ену деңгейін талдау.**

Жұмыстың практикалық маңыздылығы. Жүргізілген ғылыми зерттеулердің және алынған нәтижелердің практикалық мүмкіндігі жоғары және ақпараттық-коммуникациялық жүйелер мен желілерде құпия ақпараттарды сақтауға және алмасуда оларды қорғауға пайдалануға болады. Сонымен қатар, осы нәтижелер отандық ақпаратты қорғау құралдарын құруға, дамытуға ықпал етеді және ақпаратты шифрлаудың тиімді алгоритмдерін құру теориясын кеңейтеді. Өзірленген итеративті блоктық шифрлау алгоритмінің бағдарламалық жасақтамасы іске асырылып, ҚР Әділет министрлігі Ұлттық зияткерлік меншік институтынан «Qamal v 1.0.1» 2019 жылғы 6 қыркүйектегі № 5200 авторлық куәлігі алынды.

**5. Ресми рецензенттердің жұмысына талдау (мейлінше сапасыз пікірлерді мысалға ала отырып).**

Диссертацияның мазмұнын оқып зерделеу үшін және сыни пікір беруі үшін әрбір диссертацияға ресми түрде екі рецензент тағайындалды, олардың ғылыми дәрежелері ғылым докторы немесе ғылым кандидаты, философия (PhD) докторлары болды және докторанттың зерттеу аумағындағы ғылыми мақалалары 5 (бесеуден) аз болмауы шарт екендігі ескерілді.



Ресми рецензенттерді тағайындау кезінде диссертациялық кеңес рецензент пен докторанттың, ғылыми кеңесшілерімен бір-біріне тәуелсіз болу принципін жетекшілікке ала отырып тағайындады.

Ресми рецензенттер диссертациялық кеңеске жазбаша түрде пікірлерін көрсетті, онда диссертацияның ғылымның даму бағытына және (немесе) мемлекеттік бағдарламаларға сәйкестілігі, өзектілігі, жаңашылдық принциптеріне сәйкестілігі, автордың жеке үлесі, нақтылығы, ішкі бірлігі, практикалық маңызы, академиялық адалдылығы ескерілген және философия (PhD) докторы дәрежесін алу мүмкіншілігі қортындыланған. Ресми рецензенттердің берген пікірлерінің көшірмесі докторанттарға берілді және диссертацияны қорғау күні белгіленген күнге 5 (бес) жұмыс күні қалғанға дейін университеттің интернет ресурсына ілінді.

#### **6. Ғылыми кадрларды даярлау жүйесін одан әрі жетілдіру жөніндегі ұсыныстар.**

Жоқ.

#### **7. Философия докторы (PhD), бейіні бойынша доктор дәрежесіне ізденушілердің мамандықтар (кадрларды даярлау бағыты) бойынша қаралған диссертациялар туралы деректер:**

	6D07300, 8D06101 – Ақпараттық жүйелер	6D070400 - Есептеу техникасы және бағдарламалық қамтамасыз ету (Компьютерлік инженерия)	6D075100 - Информатика, есептеу техникасы және басқару (Жүйелік инженерия)	6D060200 - Информатика (Компьютерлік ғылымдар)	6D100200, 8D06301 - Ақпараттық қауіпсіздік жүйелері	6D070200 - Автомагтандыру және басқару
Қорғауға қабылданған диссертациялар (оның ішінде басқа ЖОО докторанттарының)	-	-	1	-	1	-
Қараудан алынып тасталған диссертациялар (оның ішінде басқа ЖОО докторанттарының)	-	-	-	-	-	-
Рецензенттердің теріс пікірін алған диссертациялар (оның ішінде басқа	-	-	-	-	-	-

ЖОО докторанттарының)						
Қорғау нәтижелері бойынша теріс шешім алған диссертациялар (оның ішінде басқа ЖОО докторанттарының)	-	-	-	-	-	-
Пысықтауға жіберілген диссертациялар (оның ішінде басқа ЖОО докторанттарының)	-	-	-	-	-	-
Қайта қорғауға жіберілген диссертациялар (оның ішінде басқа ЖОО докторанттарының)	-	-	-	-	-	-

Диссертациялық кеңестің  
төрағасы



Қалимолдаев М.Н.

Диссертациялық кеңестің  
ғалым хатшысы

Дәрібаев Б.С.

Мөр Мерзімі 2021 жыл «30» желтоқсан