

**«6D100200 – Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша философия докторы (PhD) дәрежесіне іздену үшін ұсынылған
Алғазы Күнболат Тілеуханұлының «Әртүрлі әдістерге негізделген шифрлау алгоритмдерін құру және зерттеу» тақырыбындағы
диссертациялық жұмысына ресми рецензенттің**

СЫН-ПІКІРІ

р/н №	Критерийлер	Критерийлер сәйкестігі	Ресми рецензенттің ұстанымы
1.	Диссертация тақырыбының (бекіту күніне) ғылымның даму бағыттарына және/немесе мемлекеттік бағдарламаларға сәйкес болуы	<p>1.1 Ғылымның даму бағыттарына және/немесе мемлекеттік бағдарламаларға сәйкестігі:</p> <p>1) <u>Диссертация мемлекет бюджетінен қаржыландырылатын жобаның немесе нысаналы бағдарламаның аясында орындалған (жобаның немесе бағдарламаның атауы мен нөмірі);</u></p> <p>2) Диссертация басқа мемлекеттік бағдарлама аясында орындалған (бағдарламаның атауы)</p> <p>3) Диссертация Қазақстан Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия бекіткен ғылым дамуының басым бағытына сәйкес (бағытын көрсету)</p>	<p>Диссертацияның тақырыбы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысымен бекітілген «Киберқауіпсіздік («Қазақстанның киберқалқаны») тұжырымдамасына» және 2017 жылғы 12 желтоқсандағы №827 қаулысымен бекітілген «Цифрлық Қазақстан» мемлекеттік бағдарламасына сәйкес келеді.</p> <p>Зерттеу жұмыстары мемлекет бюджетінен қаржыландырылған бағдарламалық – нысаналы қаржыландыру жобасының ғылыми-зерттеу жұмыстарының аясында орындалған. ЖТН – BR05236757-OT-20 «Жалпы мақсаттағы желілер мен инфокоммуникациялық жүйелерде ақпаратты жіберу және сақтау кезінде оны криптографиялық қорғау үшін бағдарламалық және бағдарламалық - аппараттық кешендерді құрастыру».</p>
2.	Ғылымға маңыздылығы	Жұмыс ғылымға елеулі үлесін қосады/қоспайды, ал оның маңыздылығы ашылған/ашылмаған.	Жұмыс ғылымға елеулі үлесін қосады және оның маңыздылығы жұмыста жақсы ашылған. Барлық ақпараттық және телекоммуникациялық жүйелердің нысандары мен субъектілері арасындағы ақпараттық өзара алмасу үдерісінің қауіпсіздігін қамтамасыз ету мәселесінің мәні күннен-күнге жоғарлап келеді. Сондықтан ақпараттық және телекоммуникациялық жүйелерді қолданушылардың сақтаудағы және қолданыстағы ақпараттық ресурстарына рұқсатсыз кіруден сенімді қорғау басты мәселелердің

			<p>бірі. Осының барлығы ақпараттық қауіпсіздік технологияларды және оларды жүзеге асыру құралдарын үнемі жетілдіруді және дамытуды қажет етеді. Телекоммуникация жүйелерін, желілерін және құрылғыларын зерттеу саласындағы маңызды мәселелердің бірі олардың қауіпсіздігін қамтамасыз ету және ақпаратты қорғаудың жаңа тәсілдерін әзірлеу және зерттеу болып табылады. Өз кезегінде ақпаратты қорғау мәселесі, мәліметті шифрлаумен байланысты криптографиялық тәсілдерді қолдануға негізделген. Жұмыста ақпараттарды криптографиялық қорғаудың жаңа симметриялы блоктық шифрлау алгоритмі құрылған.</p>
3.	Өзі жазу принципі	<p>Өзі жазу деңгейі:</p> <ol style="list-style-type: none"> 1) жоғары; 2) орташа; 3) төмен; 4) өзі жазбаған 	<p>Өзі жазу деңгейі жоғары. Диссертант зерттеу жұмыстарын өз бетімен орындағаны байқалады. Жұмыс мақсатына жету үшін, блоктық шифрлау алгоритмін құрып, оған жан-жақты ғылыми зерттеу жүргізген. Диссертациялық жұмыстың үшінші бөлімінде құрылған алгоритмнің криптоберіктілігі анықталып көрсетілген. Атап айтқанда, дифференциалдық, сызықтық, XL, XSL және бумеранг шабуылдарына тұрақтылығы арқылы шифрдың беріктілігін дәйектейді. Блоктық шифрға, кілт арқылы орындалатын түрлендіруде позициялы емес полиномдық санау жүйесін (ПЕПСЖ) қолдану кезіндегі ерекшеліктер көрсетілген. Осы жұмыстардың барлығы, автордың өзі жазу принципінің және деңгейінің жоғары екендігін білдіреді.</p>
4.	Ішкі бірлік принципі	<p>4.1 Диссертация өзектілігінің негіздемесі:</p> <ol style="list-style-type: none"> 1) негізделген; 2) жартылай негізделген; 3) негізделмеген. 	<p>Диссертациялық жұмыстың өзектілігі кіріспе және бірінші бөлімде негізделіп көрсетілген. Ақпараттық технологияның дамуы бір орында тұрған жоқ. Ақпарат әлемінде үздіксіз қарулану жарысы жүріп жатыр. Жаңа технологиялардың пайда болуымен қауіптер саны артып, сәйкесінше ақпаратты қорғау әдістері де дамып келеді. Ақпаратты қорғау әдістерінің бірі криптография болып табылады. Криптография – мәліметтердің құпиялылығын және тұтастығын қамтамасыз ете отырып, ақпаратты қауіпсіз түрде беруге мүмкіндік береді. Заманауи талаптарға сай криптографиялық әдістерді, оның ішінде блоктық шифрлау әдістерін құру және зерттеу өзекті болып саналады. Бұл жұмыста блоктық шифрға негізделген криптографиялық алгоритмді құру жолы және оның сенімділігі сипатталған. Зерттеу нәтижелері ұсынылған алгоритмнің жеткілікті</p>

		<p>тиімді және қауіпсіз екенін көрсетеді.</p> <p>4.2 Диссертация мазмұны диссертация тақырыбын айқындайды 1) <u>айқындайды</u>; 2) жартылай айқындайды; 3) айқындамайды</p> <p>4.3. Мақсаты мен міндеттері диссертация тақырыбына сәйкес келеді: 1) <u>сәйкес келеді</u>; 2) жартылай сәйкес келеді; 3) сәйкес келмейді</p> <p>4.4. Диссертацияның барлық бөлімдері мен құрылысы логикалық байланысқан: 1) <u>толық байланысқан</u>; 2) жартылай байланысқан; 3) байланыс жоқ</p>	<p>Диссертация мазмұны зерттеу жұмысының тақырыбын толық ашады. Диссертациялық жұмыс ақпараттарды криптографиялық қорғаудың симметриялы блоктық шифрларын әзірлеуге және оның криптоберіктілігін зерттеуге арналған. Аталған жұмыстардың барлығы диссертация тақырыбын толық айқындайды.</p> <p>Диссертацияның мақсаттары мен міндеттері тақырыбына сәйкес келеді. Жұмыстың мақсаты - позициялы емес полиномдық санау жүйесін пайдаланып итеративті блоктық шифрлау алгоритмін және раундтық кілттер алгоритмін құру және құрылған алгоритмдердің криптоберіктілігін зерттеу. Келесі зерттеу міндеттері қойылған:</p> <ul style="list-style-type: none"> - ақпаратты криптографиялық қорғаудың қолданыстағы симметриялық блоктық алгоритмдеріне сараптау жүргізу; - криптографиялық шабуылдардың және криптоталдаудың белгілі әдістерін қарастыру және талдау; - позициялық емес полиномдық санау жүйесін пайдаланып раундтық кілттер алу және ауыстыру-алмастыру желісі негізінде симметриялы блоктық шифрлау алгоритмдерін құру; - құрылған шифрлау алгоритмдерін беріктілігін криптоталдау әдістері арқылы зерттеу; - құрылған итеративті шифрлау алгоритмдерін бағдарламалық жүзеге асыру. <p>Диссертацияның барлық бөлімдері логикалық байланысқан. Кіріспеде диссертациялық жұмыс тақырыбының өзектілігінің негіздемесі, ғылыми-зерттеу жұмысының мақсаты, нысаны және пәні тұжырымдалған. Сонымен бірге, ғылыми жаңалығы және тәжірибелік маңызы көрсетілген. Бірінші бөлімде, криптографиялық алгоритмдердің түрлері және олардың қауіпсіздігінің дәрежесі бойынша бөлінген топтарына сипаттамалар келтіріліп, симметриялы блоктық шифрларға қойылатын талаптар аталған. Екінші бөлімде, SP-жүйесі негізінде құрылған жаңа шифрлау алгоритмі сипатталады және S-блок ауыстыруының құрылысы сипатталған. Сонымен бірге, «Qamal NPNS» алгоритмі ПЕПСЖ негізделген алгоритм болғандықтан, ПЕПСЖ-лерінің құрылуы және оны шифрлауда, шифрды кері ашуда қалай</p>
--	--	---	---

			<p>қолданылатыны туралы мәліметтер берілген. Үшінші бөлімде, шифрлау алгоритмінің криптоберіктілігі зерттеліп, нәтижелері берілген. Алгоритмнің беріктілігін бағалау үшін криптоталдаудың алгебралық, дифференциалдық, сызықтық және тағы басқа да әдістерімен тексерілген. Жүргізілген криптошабуылдардың теориялық бағасы ғана емес, нәтижелері нақты мысалдар арқылы да көрініс табады. Сонымен қатар, кілтті ПЕПСЖ-де пайдаланғанда алгоритмнің беріктілігіне әсері зерттелген. Төртінші бөлімде, құрылған бағдарламалық жасақтаманың бағдарламалық тілі, жүйелік талаптары, жұмыс істеу түсіндірілімдемелері және т.б. мәліметтер келтірілген. Бағдарламаның есептеу істеу жылдамдығын арттыру мақсатында шифрлау алгоритмінде қолданылған Mixer2 түрлендіруін үш тәсіл бойынша жүзеге асырылуы қарастырылып, нәтижелеріне салыстыру жүргізілген.</p>
		<p>4.5 Автор ұсынған жаңа шешімдер (қағидаттар, әдістер) дәлелденіп, бұрыннан белгілі шешімдермен салыстырылып бағаланған:</p> <ol style="list-style-type: none"> 1) <u>сыни талдау бар;</u> 2) талдау жартылай жүргізілген; 3) талдау өз пікірін емес, басқа авторлардың сілтемелеріне негізделген 	<p>Диссертацияда ұсынылған жаңа шешімдер дәлелденіп көрсетілген. Құрылған шифрлау алгоритмінің беріктілігі криптоталдаудың әдістерін қолдана отырып дәлелденіп көрсетілген. Криптоталдау талаптарына жауап беретін S-блок ауыстыру кестесі құрылып, оның сандық сипаттамалары DES, AES, Калина және Кузнечик сияқты белгілі алгоритмдердің S-блогымен салыстырылып және олардан беріктілігі кем еместігі көрсетілген.</p>
5.	Ғылыми жаңашылдық принципі	<p>5.1 Ғылыми нәтижелер мен қағидаттар жаңа болып табыла ма?</p> <ol style="list-style-type: none"> 1) <u>толығымен жаңа;</u> 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады) 	<p>Зерттеу жұмысының ғылыми нәтижелері мен қағидаттары толығымен жаңа. Ақпараттық желілер мен жүйелерді қорғауға арнап құрылған симметриялы блоктық шифрлау алгоритмі жаңа болып табылады. Сондай-ақ, позициялы емес полиномдық санау жүйесін блоктық шифрларға қолданғанда криптографиялық беріктілікке әсерін зерттеу жұмысы да және шифрлауға пайдаланылған компоненттердің бірі - S-блок ауыстыруы да өзіндік жаңа.</p>
		<p>5.2 Диссертацияның қорытындылары жаңа болып табыла ма?</p> <ol style="list-style-type: none"> 1) <u>толығымен жаңа;</u> 2) жартылай жаңа (25-75% жаңа болып табылады); 	<p>Диссертациялық жұмыста теориялық және тәжірибелік зерттеулер жүргізу нәтижесінде криптографияда кеңінен қолданылатын SP-желісіне негізделген симметриялы блоктық шифрлау алгоритмі құрылған және кілттерді қолданудағы ерекшелігіне қарай ПЕПСЖ негізделген екінші нұсқасы ұсынылған. Әзірленген алгоритмде</p>

		3) жаңа емес (25% кем жаңа болып табылады)	қолданылған түрлендірулер сипатталып, бағдарламалық жасақтамасы іске асырылған. Диссертацияның қорытындылары толығымен жаңа болып табылады.
		5.3 Техникалық, технологиялық, экономикалық немесе басқару шешімдері жаңа және негізделген бе? 1) <u>толығымен жаңа</u> ; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Диссертациялық жұмыстың техникалық және технологиялық шешімдері жаңа және негізделген. Корпоративтік инфрақұрылым мен инновациялық технологиялардың дамуымен қатар шифрлау мүмкіндіктері де кеңейіп келеді. Криптографиялық технологиялар ақпараттарды қорғау процестерінде деректердің тұтастығын қамтамасыз ету және бақылауды жүзеге асыруға мүмкіндік береді. Зерттеу жұмысы позициялы емес полиномдық санау жүйесін пайдалана отырып симметриялы блоктық шифр құру болып табылады. Блоктық шифрлар бірқатар артықшылықтарына байланысты ақпаратты криптографиялық қорғаудың негізгі технологияларының біріне айналып отыр.
6.	Негізгі қорытындылардың негізділігі	Барлық қорытындылар ғылыми тұрғыдан қарағанда ауқымды дәлелдемелерде <u>негізделген/негізделмеген</u> (qualitative research және өнертану және гуманитарлық бағыттары бойынша)	Диссертациялық жұмыстың қорытындылары жүргізілген ғылыми-зерттеу жұмыстарының нәтижелерімен негізделген. Ауыстыру-алмастыру жүйесі құрылымындағы жаңа симметриялы блоктық шифрлау алгоритмін құрып, беріктілігі зерттеліп көрсетілген. Атап айтқанда, криптографияның дифференциалдық, сызықтық, XL, XSL және бумеранг шабуылдарға қарсы тұра алатындығы дәлелденіп көрсетілген. Шифрмәтіндердің және раундтық кілттер тізбегінің статистикалық қасиеттерін тексеруде бағалау тестілерінің ішінде келесілер қолданылған: 0 мен 1-ді тексеру; байланыстырылмаған серияларды тексеру; символ бойынша тексеру; интервалдарды тексеру; комбинацияларды тексеру; купондар жинаушы тесті; алмастыруларды тексеру; монотондылықты тексеру; корреляцияны тексеру; сызықтық күрделілікті тексеру; спектрлік тест; қиылысатын ауыстыруларды тексеру. Статистикалық зерттеулер оң нәтижелер берген.
7.	Қорғауға шығарылған негізгі қағидаттар	Әр қағидат бойынша келесі сұрақтарға жауап беру қажет: 7.1 Қағидат дәлелденді ме? 1) <u>дәлелденді</u> ; 2) шамамен дәлелденді; 3) шамамен дәлелденбеді;	Диссертанттың жұмысы бйынша қорғауға шығарылған негізгі келесі қағидаттарды атауға болады: - Шифрлау алгоритмдеріне қойылатын жалпы талаптарға жауап беретін, ауыстыру-алмастыру жүйесі құрылымындағы жаңа симметриялы блоктық шифрлау алгоритмі құрылды. Қағидат дәлелденген, тривалды емес, жаңа, қолдану деңгейі кең

		<p>4) дәлелденбеді 7.2 Тривиалды ма? 1) ия; 2) <u>жок</u> 7.3 Жаңа ма? 1) <u>ия</u>; 2) жок 7.4 Қолдану деңгейі: 1) тар; 2) орташа; 3) <u>кең</u> 7.5 Мақалада дәлелденген бе? 1) <u>ия</u>; 2) жок</p>	<p>және келесі мақалада дәлелденген: K.T. Algazy, L.K. Babenko, R.G. Biyashev, E.A. Ishchukova, N.A. Kapalova, S.E. Nysynbaeva, Andrzej Smolarz Differential Cryptanalysis of New Qamal Encryption Algorithm // International journal of electronics and telecommunications, № 4, 2020, P. 647-653</p> <p>-позициялы емес полиномдық санау жүйесіне негізделген симметриялы блоктық шифрлау алгоритмі құрылды, оны қолдану алгоритмінің криптографиялық беріктігін арттыруға мүмкіндік береді; Қағидат дәлелденген, тривалды емес, жаңа, қолдану деңгейі кең және келесі мақалада дәлелденген: R.G. Biyashev, A. Smolarz, K. T. Algazy, A.Khomysh. Encryption algorithm "Qamal NPNS" based on a nonpositional polynomial notation // Вестник КазНУ им. аль-Фараби. – Алматы, 2020. – № 1. – С. 198-208.</p> <p>-дифференциалдық және сызықтық криптоталдауларға беріктілік көрсеткіштері жоғары, S-блок ауыстыру кестесі құрылды. Қағидат дәлелденген, тривалды емес, жаңа, қолдану деңгейі кең және келесі мақалаларда дәлелденген: 1. R.G. Biyashev, N.A. Kapalova, D.S. Duysenbayev, K.T. Algazy, Waldemar Wojcik, Andrzej Smolarz Development and Analysis of Symmetric Encryption Algorithm Qamal Based on a Substitution-permutation Network // International journal of electronics and telecommunications, № 1, 2021, P. 127-132 2. Бияшев Р.Г., Алгазы К.Т., Дюсенбаев Д.С., Сакан К.С. Результаты линейного криптоанализа шифра Qamal // Вестник АУЭС. – Алматы, 2020. – № 2. – С. 96-105.</p>
8.	Дәйектілік принципі Дереккөздер мен ұсынылған	<p>8.1 Әдістеменің таңдауы - негізделген немесе әдіснама нақты жазылған 1) <u>ия</u>; 2) жок</p>	<p>Диссертациялық жұмыста таңдалған әдістеме нақты жазылған және негізделген. Симметриялық алгоритмдер азырақ ресурстарды қажет етеді және асимметриялық алгоритмдерге қарағанда жылдам шифрлау жылдамдығын көрсетеді. Симметриялық шифрлардың көпшілігі теориялық тұрғыдан асимметриялық алгоритмдерге қауіп</p>

ақпараттың дәйектілігі		төндіретін кванттық компьютерлердің шабуылдарына берік. Блоктық шифрлау әдістерінің негізгі артықшылығының бірі, бір кілтті бірнеше рет қолдануға беріктілігі. Яғни, шабуылдаушыда бір кілт бойынша алынған ашық және шифр мәтіндер жұптарының саны көп болған кезде де криптоберіктілік төмендемейді. Диссертациялық жұмыста блоктық шифрлау әдісінің осы және басқа да артықшылықтары жазылған.
	8.2 Диссертация жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу және интерпретациялау әдістемелерін пайдалана отырып алынған: 1) <u>ия</u> ; 2) <u>жоқ</u>	Диссертация жұмыстың негізгі бөлімдерінің бірі болып табылатын, құрылған симметриялы блоктық шифрлау алгоритмінің сенімділігін зерттеу жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу әдістемелерін пайдалана отырып алынған. Оған дәлел, статистикалық және заманауи криптографиялық талдаудың әдістерін пайдалана отырып, ғылыми нәтижелер алған.
	8.3 Теориялық қорытындылар, модельдер, анықталған өзара байланыстар және заңдылықтар эксперименттік зерттеулермен дәлелденген және расталған (педагогикалық ғылымдар бойынша даярлау бағыттары үшін нәтижелер педагогикалық эксперимент негізінде дәлелденеді): 1) <u>ия</u> ; 2) <u>жоқ</u>	Теориялық қорытындылар статистикалық тесттердің, лавиндік эффектiнiң және криптошабуылдардың нәтижелерiмен расталған және дәлелденген. Әрбiр статистикалық тест – кiрiс тiзбегiнiң кездейсоқтығы туралы гипотезаны тексеру мәселесiн шешедi. Құрылған шифрлау алгоритмдерi үшiн графикалық және бағалау тестiлерiнен 20 түрлi форматтағы 1000 шифрланған файл үшiн жүргiзiлiп, статистикалық қасиеттерi талап етiлген деңгейге сай екендiгiн көрсеткен. Шифрдың лавиндiк эффектiсiн тексеру үшiн ұзындығы 128 бит болатын кездейсоқ ашық мәтiн тандап, әрбiр орындағы биттердi инверциялау арқылы жаңа 128 ашық мәтiн алып, оларды шифрлаған. Осы алынған шифр мәтiндердi зерттей отырып, алгоритмде лавиндiк эффектi параметрi шифрлаудың бiрiншi раундынан кейiн-ақ жақсы нәтижеге жететiндiгi көрсетiлген.
	8.4 Маңызды мәлімдемелер нақты және сенімді ғылыми әдебиеттерге сілтемелермен <u>расталған</u> / ішінара расталған / расталмаған	Диссертациялық жұмыстағы маңызды мәлімдемелер отандық және шетелдік нақты және сенімді ғылыми әдебиеттерге сілтемелер жасалған. Пайдаланған ғылыми әдебиеттер зерттеу саласына сәйкес.

		8.5 Пайдаланылған әдебиеттер тізімі әдеби шолуға <u>жеткілікті/жеткіліксіз</u>	Диссертациялық жұмыс бойынша ізденіс барысында пайдаланылған әдебиеттер тізімі әдеби шолуға жеткілікті. Олардың ішінде, Web of Science және SCOPUS халықаралық деректер қорына кірген журналдар және криптография салысында соңғы жылдары шыққан әдебиеттер бар.
9	Практикалық құндылық принципі	9.1 Диссертацияның теориялық маңызы бар: 1) <u>ия</u> ; 2) жок	Өңделетін ақпараттарға криптографиялық түрлендірулерді қолданудың теориялық маңыздылығы криптографиялық примитивтердің жаңа класын негіздеуде және блоктық алгоритмдердің итерациялық схемаларын құрудың жалпы принциптерін кеңейту және жетілдіру мүмкіндігінде жатыр. Диссертациялық жұмыстың теориялық маңызы бар, зерттеу жұмысында кілтті позициялы емес полиномдық санау жүйесінде пайдаланғанда, оның криптоберіктілікті арттыратыны дәлелденген. Сонымен қатар, жұмыс нәтижесі отандық ақпаратты қорғау құралдарын құруға және дамытуға ықпал етеді, ақпаратты шифрлаудың тиімді алгоритмдерін құру теориясын кеңейтеді.
		9.2 Диссертацияның практикалық маңызы бар және алынған нәтижелерді практикада қолдану мүмкіндігі жоғары: 1) <u>ия</u> ; 2) жок	Блоктық шифрлар көптеген криптографиялық хаттамалардың маңызды құрамдас бөлігі болып табылады және желі арқылы берілетін деректерді қорғау үшін кеңінен қолданылады. Сондықтан, құрылған шифрлау алгоритмдерін практикада қолдану мүмкіндігі жоғары.
		9.3 Практикалық ұсыныстар жаңа болып табылады? 1) <u>толығымен жаңа</u> ; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Практикалық ұсыныстар жаңа болып табылады. Ақпаратты криптографиялық қорғаудың жаңа симметриялы блоктық шифрлау алгоритмі құрылған және оны отандық ақпаратты қорғау құралдарын құруға пайдалануға болады.
10.	Жазу және ресімдеу сапасы	Академиялық жазу сапасы: 1) <u>жоғары</u> ; 2) орташа; 3) орташадан төмен; 4) төмен.	Докторлық диссертация жұмысы ғылыми тілде, сауатты жазылған және техникалық тұрғыдан дұрыс рәсімделген. Академиялық жазу сапасы жоғары. <i>Диссертациялық жұмыс бойынша келесі ескертулер мен ұсыныстарды атап өтуге болады:</i> <i>- қазақша ғылыми терминдердің баламалары кейбір жерлерде</i>

		<p>дұрыс емес. Мысалы, аспекті, классификациясы, ресурс және т.б. - жұмыста зерттеу саласы бойынша ғалымдардың еңбектері аталып өткен. Дегенмен де Ақпараттық және есептеуіш технологиялар институтында орындалған жұмыстарға талдау жасап, жұмысқа қоса кетсе артық болмас еді. Айтылған ескертулер жұмысты әрі қарай жетілдіруге нұсқаулық ретінде көрсетілген және олар диссертациялық жұмыстың құндылығын төмендетпейді.</p>
--	--	--

Ресми рецензенттер пікірлерінде келесі шешімдердің бірін көрсетеді:

1) философия докторы (PhD) немесе бейіні бойынша доктор дәрежесін беру;

Ресми рецензенттер пікірлерінің көшірмелері докторантқа диссертация қорғауға дейін кемінде 5 (бес) жұмыс күнінен кешіктірілмей беріледі.

Ресми рецензент:

Л.Н. Гумилев атындағы Еуразия ұлттық университеті
PhD, қауымдастырылған профессор

Т.К. Жукабаева

