«8D06201 – Радиотехника, электроника және телекоммуникациялар» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесіне іздену үшін ұсынылған Сқабылов Әлішер Әлиұлының «ПЛИС негізінде шифрлеуге арналған аппараттық бағдарламалық қамтамасыздандыру» 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	1.1 Ғылымның даму бағыттарына және/немесе мемлекеттік бағдарламаларға сәйкестігі:	Диссертацияда ұсынылған зерттеу нәтижелері Қазақстан Республикасы Үкіметінің жанындағы Жоғары ғылыми-техникалық комиссия бекіткен ғылымды дамытудың басым бағыттарына сәйкес келеді.
		1) Диссертация мемлекет бюджетінен қаржыландырылатын жобаның немесе нысаналы бағдарламаның аясында орындалған (жобаның немесе бағдарламаның атауы мен нөмірі); 2) Диссертация басқа мемлекеттік бағдарлама аясында орындалған (бағдарламаның атауы) 3) Диссертация Қазақстан Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия бекіткен ғылым дамуының басым бағытына сәйкес (бағытын көрсету)	Диссертациялық жұмыс Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия бекіткен ғылым дамуының, атап айтқанда "Ақпараттық, коммуникациялық және ғарыштық технологиялар" басым бағытына сәйкес келеді.
2.	Ғылымға маңыздылығы	Жұмыс ғылымға елеулі үлесін **қосады**/қоспайды, ал оның маңыздылығы **ашылған**/ашылмаған.	Жұмыс ғылымға айтарлықтай үлес қосады және оның маңыздылығы жақсы ашылған. Сқабылов Әлішер Әлиұлының диссертациялық жұмысы телекоммуникациялық жүйелерде шифрлаудың жоғары жылдамдығы мен сенімділігін қамтамасыз ететін программаланатын логикалық интегралдық схемалар (ПЛИС) көмегімен мәліметтерді аппараттық-бағдарламалық шифрлау әдістерін әзірлеуге бағытталған. Мәліметтерді қорғауды жақсартатын псевдокездейсоқ сандарды жасау үшін хаос генераторларын пайдалануға ерекше назар аударылады. Бұл әдістер ақпараттық қауіпсіздік деңгейін арттырады және жаһандық цифрландыру дәуірінде технологиялық тәуелсіздікке ықпал етеді. Жұмыс заманауи ақпараттық жүйелерде мәліметтерді

			қорғаудың жетілдірілген тәсілдерін ұсына отырып, ақпараттық қауіпсіздіктің теориялық және практикалық аспектілерін айтарлықтай байытады.
3.	Өзі жазу принципі	Өзі жазу деңгейі: 1) **жоғары**; 2) орташа; 3) төмен; 4) өзі жазбаған	Ізденуші орындаған жұмыс дербес зерттеу болып табылады. Диссертацияда келтірілген барлық тәжірибелік мәліметтерді автор өз бетінше алған. Диссертациялық жұмыста ғылыми әдебиеттерді орынды, сауатты қолдана білген. Диссертация мәтінінде келтірілген суреттер мен кесте түріндегі мәліметтердің жаңа, әрі түпнұска екендігі байқалады.
4.	Ішкі бірлік принципі	4.1 Диссертация өзектілігінің негіздемесі: 1) **негізделген**; 2) жартылай негізделген; 3) негізделмеген.	Диссертациялық жұмыстың өзектілігі нақты көрсетілген және жұмыста алынған нәтижелер күмән тудырмайды. Зерттеу тақырыбы бойынша әдебиеттерге шолу ізденушінің осы бағытта зерттеліп жатқан жұмыстарды және диссертация тақырыбы бойынша мәселенің қазіргі жағдайын жақсы білетінін көрсетеді.
		4.2 Диссертация мазмұны диссертация тақырыбын айқындайды 1) **айқындайды**; 2) жартылай айқындайды; 3) айқындамайды	Диссертациялық жұмыстың мазмұны тиянақты және диссертация тақырыбы бойынша зерттеудің мақсаты мен міндеттерін толық қамтиды.
		4.3. Мақсаты мен міндеттері диссертация тақырыбына сәйкес келеді: 1) **сәйкес келеді**; 2) жартылай сәйкес келеді; 3) сәйкес келмейді	Ә.Ә. Сқабыловтың қойған мақсаты мен міндеттері диссертация тақырыбына толығымен сәйкес келеді.
		4.4. Диссертацияның барлық бөлімдері мен құрылысы логикалық байланысқан: 1) **толық байланысқан**; 2) жартылай байланысқан; 3) байланыс жоқ	Диссертациялық жұмыстың барлық бөлімдері мен ғылыми тұжырымдары өзара толықтай байланысқан, мақсаты мен міндеттерін шешуге бағытталған. Зерттеу нысандары, зерттеу әдістерінің сипаттамалары келтірілген.
		4.5 Автор ұсынған жаңа шешімдер (қағидаттар, әдістер) дәлелденіп, бұрыннан белгілі шешімдермен салыстырылып бағаланған: 1) **сыни талдау бар**; 2) талдау жартылай жүргізілген;	Белгілі әрі жеткілікті деңгейде зерттелмеген мәселелерге сыни талдау арқылы автор диссертациялық жұмысында қойылған мақсаты мен міндеттерін және зерттеу нәтижелерін алу әдістерін көрсететін өз қағидаттарын ұсынған және тәжірибе жүзінде дәлелдеген.

		3) талдау өз пікірін емес, басқа авторлардың сілтемелеріне негізделген	
5.	Ғылыми жаңашылдық принципі	5.1 Ғылыми нәтижелер мен қағидаттар жаңа болып табыла ма? 1) **толығымен жаңа**; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Докторанттың ұсынған ғылыми нәтижелері мен тұжырымдарының жаңалығы бар деп санаймын. Сқабылов Әлішер Әлиұлының диссертациясында ұсынылған ғылыми нәтижелер мен тұжырымдамалар ПЛИС негізінде мәліметтерді шифрлау әдістерін, соның ішінде позициялық емес көпмүшелік санау жүйесін (ПЕКСЖ) және псевдокездейсоқ сандарды құру үшін хаос генераторларын қолдануды енгізеді. Жұмыс сонымен қатар шифрлау алгоритмдерінде қолдану үшін келтірілмейтін көпмүшеліктердің деректер қорын әзірлеуді және жүйелеуді қамтиды, бұл криптография саласына айтарлықтай толықтыру болып табылады. Бұл әдістер мәліметтерді өңдеудің сенімділігі мен жылдамдығының жоғарылауын қамтамасыз етеді.
		5.2 Диссертацияның қорытындылары жаңа болып табыла ма? 1) **толығымен жаңа**; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Қорғауға ұсынылған диссертациялық жұмыстың қорытындылары толығымен жаңа болып табылады. Алынған нәтижелер ғылыми басылымдарда жарияланған ғылыми мақалалар мен конференция материалдарымен расталған.
		5.3 Техникалық, технологиялық, экономикалық немесе басқару шешімдері жаңа және негізделген бе? 1) **толығымен жаңа**; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Техникалық, әдістемелік және басқару шешімдері толықтай жаңа және негізделген.
6.	Негізгі қорытындылар-дың негізділігі	Барлық қорытындылар ғылыми тұрғыдан қарағанда ауқымды дәлелдемелерде **негізделген**/негізделмеген (qualitative research және өнертану және гуманитарлық бағыттары боынша)	Диссертациялық жұмыста келтірілген тұжырымдар ғылыми тұрғыдан сандық нәтижелермен және теориялық мәліметтер мен басқа да жұмыстармен салыстыру әдісі арқылы дәлелденген. Жұмыс тиянақты, түсінікті және тәжірибелік дәлелдермен жазылған, таңдалған әдістер, алынған нәтижелер негізделген.
7.	Қорғауға шығарылған	Әр қағидат бойынша келесі сұрақтарға жауап беру қажет:	7.1 Қорғауға шығарылатын негізгі қағидаттар диссертацияда ұсынылған нәтижелермен дәлелденеді.

	негізгі қағидаттар	7.1 Қағидат дәлелденді ме? 1) **дәлелденді**; 2) шамамен дәлелденді; 3) шамамен дәлелденбеді; 4) дәлелденбеді 7.2 Тривиалды ма? 1) ия; 2) **жоқ** 7.3 Жаңа ма? 1) **ия**; 2) жоқ 7.4 Қолдану деңгейі: 1) тар; 2) орташа; 3) **кең** 7.5 Мақалада дәлелденген бе? 1) **ия**; 2) жоқ	7.2 Диссертациялық жұмыста тривиалдылық жоқ. Тәжірибе барысында алынған барлық заңдылықтар мен ерекшеліктер заманауи ғылыми әдістерге және мәліметтерге негізделген. 7.3 Қорғауға шығарылатын қағидаттар жаңа болып табылады. 7.4 Қолдану деңгейі кең. 7.5 Диссертациялық жұмыс материалдары негізінде 10 баспа жұмысы, оның ішінде Қазақстан Республикасы ҒЖБМ ҒЖБССҚК ұсынған басылымдарда 3 мақала, Web of Science (Clarivate Analytics) және Scopus халықаралық ақпараттық ресурстарына кіретін импакт-факторы жоғары журналдарда 2 мақала және Халықаралық ғылыми конференцияларында 5 жұмыс жарияланған.
8.	Дәйектілік принципі Дереккөздер мен ұсынылған ақпараттың дәйектілігі	8.1 Әдістеменің таңдауы - негізделген немесе әдіснама нақты жазылған 1) **ия**; 2) жоқ	Диссертациялық жұмыста қолданылған әдістер мен әдістемелік тәсілдер толығымен сипатталған. Әртүрлі деректер көздеріне жан-жақты шолу жасалған.
		8.2 Диссертация жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу және интерпретациялау әдістемелерін пайдалана отырып алынған: 1) **ия;** 2) жоқ	Сқабылов Әлішер Әлиұлының диссертациялық жұмысында ғылыми зерттеулер мен мәліметтерді өңдеудің озық әдістері мен құралдары пайдаланылды. Атап айтқанда, Matlab хаос генераторын әзірлеу және сынау үшін пайдаланылды, бұл оның параметрлерін дәл талдауға және псевдокездейсоқ сандарды жасау үшін оңтайландыруға мүмкіндік береді. Artyx-7 ПЛИС көмегімен шифрлау функциясы жүзеге асырылды және әдістерді жетілдіру үшін қолданылатын келтірілмейтін көпмүшелердің мәліметтер базасы құрылды.
		8.3 Теориялық қорытындылар, модельдер, анықталған өзара байланыстар және заңдылықтар эксперименттік зерттеулермен дәлелденген және расталған (педагогикалық ғылымдар бойынша	Диссертациялық жұмыстағы теориялық қорытындылар, модельдер, анықталған өзара байланыстар және заңдылықтар өзіндік зерттеулерімен дәлелденген және ғылыми жарияланымдарда бар болуымен расталады.

		даярлау бағыттары үшін нәтижелер педагогикалық эксперимент негізінде дәлелденеді): 1) **ия;** 2) жоқ	
		8.4 Маңызды мәлімдемелер нақты және сенімді ғылыми әдебиеттерге сілтемелермен **расталған** / ішінара расталған / расталмаған	Ә.Ә. Сқабыловтың диссертациялық жұмысындағы барлық негізгі, маңызды мәлімдемелер ғылыми әдебиетке сілтемелермен расталған.
		8.5 Пайдаланылған әдебиеттер тізімі әдеби шолуға **жеткілікті**/жеткіліксіз	Диссертациялық жұмыста пайдаланылған әдебиет тізімі 117. Барлық әдеби дереккөздер ғылыми өзекті материалдарды қамтиды және диссертация тақырыбына аналитикалық әдеби шолу жүргізуге жеткілікті.
9	Практикалық құндылық принципі	9.1 Диссертацияның теориялық маңызы бар: 1) **ия**; 2) жоқ	Диссертациялық жұмыстың теориялық маңыздылығы жоғары. Зерттеу барысында алынған нәтижелер электрондық газ сенсорларының сезімтал элементі ретінде қолданылатын шалаөткізгіштік наноқұрылымдарды алудың тиімді технологиялық параметрлерін ұсынады.
		9.2 Диссертацияның практикалық маңызы бар және алынған нәтижелерді практикада қолдану мүмкіндігі жоғары: 1) **ия;** 2) жоқ	Сқабылов Әлішер Әлиұлының диссертациясы ПЛИС негізіндегі шифрлау әдістерін жасау арқылы ақпараттық қауіпсіздіктің теориялық аспектілеріне үлкен үлес қосады. Бұл зерттеу мәліметтерді шифрлауда программаланатын логикалық интегралды схемаларды қолдануды түсінуді жақсартады және телекоммуникациялық жүйелердің қауіпсіздігін арттырудың теориялық негіздерін нығайтады.
		9.3 Практикалық ұсыныстар жаңа болып табылады? 1) **толығымен жаңа**; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Практикалық ұсыныстар толығымен жаңа. Осыған дейінгі зерттеу жұмыстарында мұндай мәліметтер келтірілмеген.
10.	Жазу және ресімдеу сапасы	Академиялық жазу сапасы: 1) **жоғары**; 2) орташа; 3) орташадан төмен; 4) төмен.	Диссертациялық жұмыс сауатты ғылыми-техникалық тілде, түсінікті стильде жазылған және оңай оқылады. Негізгі тұжырымдар сенімді және толықтай аяқталған.

Философия докторы (PhD) дәрежесін беру мүмкіндігі туралы қорытынды.

Сқабылов Әлішер Әлиұлының **«ПЛИС негізінде шифрлеуге арналған аппараттық бағдарламалық қамтамасыздандыр»** тақырыбындағы диссертациялық жұмысы жоғары ғылыми деңгейде орындалған, толығымен аяқталған және өзіндік ғылыми зерттеу сипатына ие. Диссертациялық жұмыс мазмұны мен рәсімделуі бойынша, Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым және жоғары білім саласындағы сапаны қамтамасыз ету комитетінің (ҒЖБМ ҒЖБССҚК) қоятын талаптарына толық сәйкес келеді және алынған нәтижелер халықаралық журналдарда жарияланған. Сқабылов Әлішер Әлиұлының «8D06201 – Радиотехника, электроника және телекоммуникациялар» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесіне лайық деп есептеймін.

Ресми рецензент:
С. Сейфуллин атындағы Қазақ агротехникалық Зерттеу Университеті,
радиотехника, электроника және телекоммуникациялар кафедрасы,
PhD, қауымдастырылған профессор

Медетов Б.Ж.