**«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: | «Техника ғылымдары саласындағы ғылыми зерттеулер мен әзірлемелер» ғылымды дамытудың басым бағытына сәйкес келеді. |
| | | 1) Диссертация мемлекет бюджетінен қаржыландырылатын жобаның немесе нысаналы бағдарламаның аясында орындалған (жобаның немесе бағдарламаның атауы мен нөмірі);<br>2) Диссертация басқа мемлекеттік бағдарлама аясында орындалған (бағдарламаның атауы)<br>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. | Диссертациялық жұмыста жұмыста келтірілген деректер ғылымға маңызды үлес қосуда. Ол жаңа, ғылыми негізделген нәтижелерді көрсетеді, оларды қолдану маңызды қолданбалы мәселелерді шешуге ықпал етеді. ПЛИС негізіндегі аппараттық және бағдарламалық мәліметтерді шифрлау әдістерін дамыту телекоммуникациялық жүйелердегі мәліметтерді өңдеудің күшейтілген қауіпсіздігі мен тиімділігін арттырады. Псевдокездейсоқ сандарды жасау үшін хаос |

| | | | |
|---|---|---|---|
| | | | генераторларын пайдалану шифрлау жүйелерінің күшін арттырады, бұл оларды шабуылдарға осал етеді. Бұл әдістер заманауи ақпараттық желілерде ақпараттың құпиялылығы мен тұтастығын қамтамасыз ету арқылы мәліметтерді қорғауды айтарлықтай жақсартады. |
| 3. | Өзі жазу принципі | Өзі жазу деңгейі:<br>1) жоғары;<br>2) орташа;<br>3) төмен;<br>4) өзі жазбаған | Автор диссертациялық жұмыстың барлық бөлімін, жұмыстың мақсаты мен міндеттерін айқындауды, әдістемелерді қоюды және тәжірибелік жұмыстар жүргізуді, сондай-ақ, тәжірибе нәтижелерін өңдеп ғылыми жарияланымдарға дайындауды толығымен өзі орындаған. |
| 4. | Ішкі бірлік принципі | 4.1 Диссертация өзектілігінің негіздемесі:<br>1) негізделген;<br>2) жартылай негізделген;<br>3) негізделмеген. | Сқабылов Ә.Ә.-ның иссертациялық жұмысының өзектілігін негіздеу деректерді қорғау деңгейін арттыру үшін қазіргі заманғы ақпараттық жүйелердің өсіп келе жатқан қажеттілігінде жатыр. Ақпараттық қауіптердің артуы және ақпараттық технологиялар қауіпсіздігіне талаптардың өсуі жағдайында деректерді қорғаудың тиімділігі мен сенімділігі технологиялық тәуелсіздік пен ұлттық қауіпсіздікті қамтамасыз етудің негізгі факторларына айналуда. Сқабылов Әлішер Әлиұлының жұмысы жоғары өнімділік пен қауіпсіздікті қамтамасыз ету үшін ПЛИС көмегімен шифрлаудың озық әдістерін әзірлеуге және енгізуге бағытталған. Хаос генераторлары мен ПЕКСЖ пайдалануға негізделген тәсіл жүйелердің криптографиялық беріктігін арттыруға арналған шешімдерді ұсынады, бұл бұл зерттеуді әсіресе ақпараттық қауіпсіздік саласы үшін өзекті етеді. |
| | | 4.2 Диссертация мазмұны диссертация тақырыбын айқындайды<br>1) айқындайды;<br>2) жартылай айқындайды;<br>3) айқындамайды | Диссертациялық жұмыстың мазмұны тақырыбына сай және ондағы келтірілген бөлімдер, бөлімшелер, қорытынды, тұжырымдар мен шешімдер бір-бірімен үйлесімді. |
| | | 4.3. Мақсаты мен міндеттері диссертация тақырыбына сәйкес келеді:<br>1) сәйкес келеді; | Жұмыстың мақсаты мен міндеттері диссертация тақырыбына сәйкес келеді. |

| | | | |
|---|---|---|---|
| | | 2) жартылай сәйкес келеді;<br>3) сәйкес келмейді | |
| | | 4.4. Диссертацияның барлық бөлімдері мен құрылысы логикалық байланысқан:<br>1) толық байланысқан;<br>2) жартылай байланысқан;<br>3) байланыс жоқ | Диссертацияның барлық бөлімдері мен құрылысы логикалық түрде өзара байланысқан және қойылған мақсаты мен міндеттерін шешуге бағытталған. |
| | | 4.5 Автор ұсынған жаңа шешімдер (қағидаттар, әдістер) дәлелденіп, бұрыннан белгілі шешімдермен салыстырылып бағаланған:<br>1) сыни талдау бар;<br>2) талдау жартылай жүргізілген;<br>3) талдау өз пікірін емес, басқа авторлардың сілтемелеріне негізделген | Диссертацияда келтірілген нәтижелер мен тұжырымдар ғылыми негізделген. Барлық мәліметтер толықтай дәлелдемелермен қамтамасыз етілген. Белгілі шешімдерге талдау жүргізілген. Сыни талдау бар. |
| 5. | Ғылыми жаңашылдық принципі | 5.1 Ғылыми нәтижелер мен қағидаттар жаңа болып табыла ма?<br>1) толығымен жаңа;<br>2) жартылай жаңа (25-75% жаңа болып табылады);<br>3) жаңа емес (25% кем жаңа болып табылады) | Диссертацияда келесі ғылыми нәтижелер мен тұжырымдамалар жаңа болып табылады:<br>- Бұл зерттеуде Artix-7 ПЛИС-та іске асырылған, 16-биттік кілттерді шығаруға қабілетті келтірілмейтін көпмүшелік генератор құрылды.<br>- - Сонымен қатар, ПЛИС негізінде хаостық сигналдар генераторларын және псевдокездейсоқ сандарды енгізу шифрланған ақпараттың криптографиялық күшін айтарлықтай арттырады. Эффект таратушы және қабылдаушы құрылғылардағы ақпараттық блоктардың ұзындығын кездейсоқ бөлу арқылы жүзеге асырылады, бұл кез-келген рұқсатсыз қол жеткізу және талдау әрекеттерін қиындатады.<br>- Сонымен қатар, ПЛИС-та ашық кілтті шифрлау алгоритмін аппараттық іске асыру параллель және конвейерлік есептеу әдістерін қолданудың арқасында бір сағат ішінде 6,239 наносекундты өңдеудің керемет жылдамдығын көрсетеді. Бұл |

| | | | |
|---|---|---|---|
| | | | мәліметтерді беру жылдамдығы мен қауіпсіздігі бойынша осы технологияны тиімді бөліп көрсете отырып, шифрлау және дешифрлеу процестерін едәуір жеделдетуді қамтамасыз етеді. |
| | | 5.2 Диссертацияның қорытындылары жаңа болып табыла ма?<br>1) толығымен жаңа;<br>2) жартылай жаңа (25-75% жаңа болып табылады);<br>3) жаңа емес (25% кем жаңа болып табылады) | Қорғауға ұсынылған диссертациялық жұмыстың қорытындылары толығымен жаңа болып табылады. |
| | | 5.3 Техникалық, технологиялық, экономикалық немесе басқару шешімдері жаңа және негізделген бе?<br>1) толығымен жаңа;<br>2) жартылай жаңа (25-75% жаңа болып табылады);<br>3) жаңа емес (25% кем жаңа болып табылады) | Техникалық, технологиялық, экономикалық немесе 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 бойынша) | Барлық қорытындылар ғылыми тұрғыдан қарағанда ауқымды дәлелдемелерде негізделген. |
| 7. | Қорғауға шығарылған негізгі қағидаттар | Әр қағидат бойынша келесі сұрақтарға жауап беру қажет:<br>7.1 Қағидат дәлелденді ме?<br>1) дәлелденді;<br>2) шамамен дәлелденді;<br>3) шамамен дәлелденбеді; | **Қағидат 1**<br>1. Аппараттық қорғаныста қолдануға арналған келтірілмейтін көпмүшелер генераторы ПЛИС Artix-7 құрылғысы арқылы 16 биттік кілтті жасауды қамтамасыз етеді.<br>7.1 дәлелденді |

| | | | |
|---|---|---|---|
| | | 4) дәлелденбеді<br>7.2 Тривиалды ма?<br>1) ия;<br>2) жоқ<br>7.3 Жаңа ма?<br>1) ия;<br>2) жоқ<br>7.4 Қолдану деңгейі:<br>1) тар;<br>2) орташа;<br>3) кең<br>7.5 Мақалада дәлелденген бе?<br>1) ия;<br>2) жоқ | 7.2 жоқ<br>7.3 ия<br>7.4 кең<br>7.5 ия<br><br>**Қағидат 2**<br>2. ПЛИС негізінде жүзеге асырылатын хаостық сигналдар мен псевдокездейсоқ сандар генераторлары жіберуші және қабылдаушы құрылғылардағы ақпараттық блоктардың ұзындығын кездейсоқ бөлу арқылы шифрланған ақпараттың крипто-төзімділігін арттырады.<br><br>7.1 дәлелденді<br>7.2 жоқ<br>7.3 ия<br>7.4 кең<br>7.5 ия<br><br>**Қағидат 3**<br>3. Паралельді және конвейерлі есептеу әдістерінің арқасында ПЛИС негізіндегі ашық кілтті шифрлау алгоритмін аппараттық іске асырудың жылдамдығы бір тактыні 6,239 нс. дейін жеткізуге болады.<br><br>7.1 дәлелденді<br>7.2 жоқ<br>7.3 ия<br>7.4 кең<br>7.5 ия |
| 8. | Дәйектілік принципі Дереккөздер мен ұсынылған | 8.1 Әдістеменің таңдауы - негізделген немесе әдіснама нақты жазылған<br>1) ия;<br>2) жоқ | Диссертацияда қолданылған әдістеме негізделген және жеткілікті түрде сипатталған. |

| | | | |
|---|---|---|---|
| | ақпараттың дәйектілігі | 8.2 Диссертация жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу және интерпретациялау әдістемелерін пайдалана отырып алынған:<br>1) ия;<br>2) жоқ | Диссертациялық жұмыстың нәтижелері ғылыми зерттеулердің қазіргі заманғы әдістері мен компьютерлік технологияларын қолдану арқылы алынды. Атап айтқанда: Artix-7, Matlab simulink. |
| | | 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):<br>1) ия;<br>2) жоқ | Теориялық қорытындылар, анықталған өзара байланыстар және заңдылықтар тәжірибелік зерттеулермен дәлелденген. Алынған нәтижелер Қазақстандық және басқа да шет елдердегі жарияланымдармен расталады. |
| | | 8.4 Маңызды мәлімдемелер нақты және сенімді ғылыми әдебиеттерге сілтемелермен расталған / ішінара расталған / расталмаған | Диссертациялық жұмыста пайдаланылған маңызды мәлімдемелер өзекті және сенімді ғылыми әдебиеттерге сілтемелермен расталған. |
| | | 8.5 Пайдаланылған әдебиеттер тізімі әдеби шолуға жеткілікті/жеткіліксіз | Пайдаланылған әдебиеттер тізімі әдеби шолуға жеткілікті. Диссертациялық жұмыста 117 ғылыми жұмысқа сілтеме жасалған. |
| 9 | Практикалық құндылық принципі | 9.1 Диссертацияның теориялық маңызы бар:<br>1) ия;<br>2) жоқ | Диссертацияның теориялық маңыздылығы бар. Осыған дейінгі зерттеу жұмыстарында мұндай мәліметтер келтірілмеген. |
| | | 9.2 Диссертацияның практикалық маңызы бар және алынған | Докторант Ә. Ә. Сқабыловтың диссертациялық жұмысында жүргізілген зерттеулердің нәтижелері қазіргі заманғы телекоммуникациялық және қауіпсіз Ақпараттық жүйелерді |

| | | | |
|---|---|---|---|
| | | нәтижелерді практикада қолдану мүмкіндігі жоғары:<br>1) ия;<br>2) жоқ | әзірлеу және жетілдіру кезінде пайдаланудың жоғары мүмкіндігіне ие. Бұл нәтижелер қаржылық транзакциялар, мемлекеттік басқару және жеке ақпаратты қорғау сияқты маңызды қосымшалардағы деректердің қауіпсіздігін арттыру үшін қолданылуы мүмкін. |
| | | 9.3 Практикалық ұсыныстар жаңа болып табылады?<br>1) толығымен жаңа;<br>2) жартылай жаңа (25-75% жаңа болып табылады);<br>3) жаңа емес (25% кем жаңа болып табылады) | Диссертациялық жұмыста қол жеткізген ғылыми-зерттеу нәтижелері мен практикалық ұсыныстары толығымен жаңа. |
| 10. | Жазу және ресімдеу сапасы | Академиялық жазу сапасы:<br>1) жоғары;<br>2) орташа;<br>3) орташадан төмен;<br>4) төмен. | Диссертациялық жұмыс қазақ тілінде түсінікті әрі сауатты жазылған. Ешқандай түсінбеушілік туғызатын жағдайлар орын алмаған және талаптарға сай рәсімделген. |

Жоғарыда қарастырылған негіздерге сүйене отырып Сқабылов Әлішер Әлиұлына «8D06201 – Радиотехника, электроника және телекоммуникациялар» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесін беруді ұсынамын.

**Ресми рецензент:**
Қ. И. Сәтбаев атындағы Қазақ ұлттық
техникалық зерттеу университеті,
Электроника, телекоммуникациялар және
ғарыштық технологиялар кафедрасының
PhD, профессоры

HR қызметі

Смайлов Н.К.