«6D100200 – Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша PhD дәрежесін алу үшін Хомпыш Ардабектің **«Позициялық емес санау жүйесін қолдану арқылы ақпаратты қорғау алгоритмін құру және зерттеу»** тақырыбындағы диссертациялық жұмысына отандық ғылыми кеңесшісі, т.ғ.к., Н.А. Капалованың

ПІКІРІ

«Цифрлық Қазақстан» мемлекеттік бағдарламасы – бұл цифрлық технологияларды қолдану есебінен елдің әрбір азаматының тұрмыс деңгейін арттыруды көздейтін маңызды кешенді бағдарлама. Ал цифрландырудың ең басты элементтерінің бір ол ақпарат екендігін ескерсек, онда ақпараттың және ақпаратты жіберу кезеңінде олардың қауіпсіздігін ұйымдастыру өзекті мәселелердің бірі. Сонымен қатар елімізде Киберқауіпсіздік «Қазақстанның киберқалқаны» тұжырымдамасы ұсынылған. Мемлекет тарапынан ұсынылып отырған осындай бағдарламалардың ең басты мақсаты заманауи ғылым мен технологиялардың мүмкіндіктерін қолдана отырып заман талабына сай келетін ақпараттық қоғам қалыптастыру. Ал ақпараттық қоғамда ақпараттың қауіпсіздігін қамтамасыз ету өзекті мәселелердің бірі.

Дамыған мемлекеттерде ақпаратты криптографиялық қорғаудың мемлекеттік стандартына сай келетін өзіндік ақпаратты қорғау алгоритмдері бар екендігі белгілі, ол өз кезегінде сенімді мемлекет қалыптастырады. Ақпараттық қоғамға аяқ басқан Қазақстан үшін ақпаратты қорғаудың заманауи талаптарын қанағаттандыратын шифрлау алгоритмдерін құру өзекті мәселелердің бірі. Көптеген отандық ғалымдар осы бағыттағы есептерді тиімді шешуде. Осы мәселелерді ескере отырып А. Хомпыш диссертациялық жұмысты жасау барысында заманауи ақпараттарды қорғау алгоритмдеріне, шетелдік және отандық ғалымдардың еңбектеріне талдау жүргізді.

Диссертациялық жұмысты зертеу нәтижесінде А.Хомпыш ақпараттарды криптографиялық қорғаудың жаңа симметриялық блокты EMCipher шифрлау алгоритмін ұсынды. Құрылған алгоритмде EM түрлендіру әдісі, S-блок ауыстыру кестесі, модуль екі бойынша қосу, цикльдық жылжыту операциясы, P-блок алмастыру түрлендірулері қолданылды. Алгоритмге қолданылған S-блок ауыстыру кестесін алудың жаңа математикалық әдісі, рауңдық кілттерді жасау алгоритмі ұсынылды, ал алгоритмнің шифрлау жылдамдығын арттыру мақсатында позициялық емес полиномды санау жүйесі (ПЕПСЖ), таңдап алған жұмыс негіздерінің индекс кестесі қолданылды. Сонымен қатар құрылған алгоритмнің криптоберіктілігі бағаланды. Құрылған симметриалық болктық алгоритмнің статистикалық қауіпсіздігі мен биттік шашырау критерийлері бағаланып, сызықты және дифференциалды криптоталдау әдістері арқылы зерттелді.

Алгоритмнің ең маңызды түрлендірулерінің бірі S-блок ауыстыру кестесіне сызықты және дифференциалды криптоталдау жүргізіліп, нәтижесі заманауи алгоримдермен салыстырылып жақсы нәтиже көрсететіндігі анықталды.

Зерттеу жұмыстарын жүргізу барысында алынған ғылыми жағалықтар жоғары рейтингті журналдарда жарияланды. Диссертациялық жұмыс нәтижелері бойынша жарияланған мақалалар – 14. Оның ішінде: THOMSON REUTERS және SCOPUS халықаралық деректер қорына кірген журналдарға жарияланған мақала – 1, Қазақстан Республикасы Білім және ғылым министрлігінің Білім және ғылым саласындағы бақылау комитеті ұсынған ғылыми баспаларда жарияланған мақалалар – 6, Қазақстан мен шетелдердегі халықаралық ғылыми конференциялар жинақтарында жарияланған мақалалар – 7.

Диссертациялық зерттеу нәтижелері ғылыми және тәжірибелік маңызы бар, оларды пайдалану елдің цифрлық әлеуетін дамыту үшін маңызды ақпаратты қорғау мәселелерін шешуді қамтамасыз етеді.

Докторантурада оқыған жылдары ізденуші А.Хомпыштың қойылған ғылыми міндеттерді өз бетінше орындап, оны уақытылы толық шеше алды. Ол ғылыми зерттеу жұмысын жүзеге асыру барысында өзінің кәсібилігімен, қойған міндеттерге жауапкершілікпен қарайтындығымен және дербестігімен ерекшеленді.

Диссертатциялық жұмысты орындау барысында алынған нәтижелер ҚР БҒМ Ақпараттық және есептеуіш технологиялар институтының Ақпараттық қауіпсіздік зертханасында талқыланып, ҚР БҒМ БК бағдарламалық-нысаналы қаржыландыру (БНҚ), BR05236757 - «Жалпы мақсаттағы желілер мен инфокоммуникациялық жүйелерде ақпаратты жіберу және сақтау кезінде оны криптографиялық қорғау үшін бағдарламалық және бағдарламалық-аппараттық кешендерді құрастыру» атты жобада жүзеге асырылды, нәтижелері БНҚ жобасының 2019-2020 жылдарға арналған есептеріне енгізілген.

Жоғарыда айтылғандарды ескере отырып, «Позициялық емес санау жүйесін қолдану арқылы ақпаратты қорғау алгоритмін құру және зерттеу» тақырыбында жазылған Хомпыш Ардабектің диссертациялық жұмысы ҚР БҒМ білім және ғылым саласындағы бақылау комитетінің «Ғылыми дәрежесін беру ережелері» (PhD) докторлық диссертацияларға қоятын барлық талаптарына толық сәйкес келеді, ал зерттеу жұмысының авторы «6D100200 – Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша PhD философия докторы ғылыми дәрежесін алуға лайықты деп есептеймін.

Отандық ғылыми кеңесші
Ақпараттық және есептеуіш технологиялар
институтының жетекші ғылым қызметкер,
т.ғ.к., ХАА академигі Н.А.Капалова

т.ғ.к Н.А.Капалованың қолын **«Растаймын»**
Ақпараттық және есептеуіш технологиялар
институтының бас ғылыми хатшысы, доктор PhD О.А. Усатова

КҰӘЛАНДЫРАМЫН
КАДР ИНСПЕКТОРЫ
УДОСТОВЕРЯЮ
СТ. ИНСПЕКТОР ОК