«6D100200 – Ақпараттық қауіпсіздік жүйелері» мамандығының PhD докторанты Хомпыш Ардабектің
«Позициялық емес санау жүйесін қолдану арқылы ақпаратты қорғау алгоритмін құру және зерттеу» тақырыбындағы диссертациялық жұмысына

АҢДАТПА

Зерттеу тақырыбының өзектілігі. Бүгінгі таңда Қазақстан индустриялық қоғамнан қазіргі ғылыми-технологиялық революцияның қатаң талаптарымен айқындалатын қоғамдық және экономикалық дамудың түбегейлі жаңа деңгейіне көшудің тарихи қажеттілігіне тап болып отыр. Себебі көптеген дамыған елдерде ақпараттық қоғам мен ақпараттық экономиканың жоғары деңгейде дамығанын ескерсек, онда Қазақстанда бұл мәсселелерді қалыптастыру өзекті мәселелердің бірі. Ал ақпараттық қоғамда оның материалдық базасы ақпараттық экономика болып табылса, маңыздылығы ақпараттық ресурсқа ауысады. Бұл жағдайда ақпараттық ресурстар рұқсат етілмеген басқа пайдаланушылардан тұрақты қорғауды қажет ететін елдің стратегиялық ресурстары ретінде қарастырылады.

Автоматтандырудың жоғары дәрежесі, компьютерлік жүйелердің адам қызметінің әртүрлі салаларына деструктивті кеңінен енгізілуі деректерді өңдеудің автоматтандырылған жүйелерін әртүрлі іс-әсерлерге қатысты өте осал етеді және қоғамды пайдаланылатын ақпараттық технологиялардың қауіпсіздік деңгейіне тәуелді етеді. Сондықтан ол арқылы таралатын ақпараттың қауіпсіздігі кез-келген компьютерлік жүйенің күрделілігі мен мақсатына қарамастан маңызды сипаттамасына айналады.

Сонымен қатар кез-келген мемлекеттің даму стратегиясында басым бағыттарының бірі ұлттық қауіпсіздік екендігін ескерсек, онда оның ең маңызды элементтерінің бірі ақпараттық қауіпсіздік болып табылады. Сондықтан ақпараттық қауіпсіздіктің жаңа технологияларын құру мәселесін шешу, оған қолжетімділікті шектеп, ақпаратты қорғаудың қажетті деңгейін қамтамасыз ету заманауи талаптарға сай келетін ақпараттық қауіпсіздік құралдарын құру өзекті мәселелердің бірі.

«Қазақстанның киберқалқаны» киберқауіпсіздік тұжырымдамасында «Зерттеулерге және қолданбалы математика, ақпаратты криптографиялық қорғау құралдарын әзірлеу, криптология, бағдарламаланатын логикалық интегралдық схемалар бойынша әзірлемелер, кванттық криптография мен ақпарат берудің, өңдеудің және сақтаудың қорғалған жүйелерін, сондай-ақ ақпараттық қауіпсіздік жүйелерін құру бойынша өз мектептерімізге басымдық беру керек» және «Отандық әзірлемелердің сұранысқа аса ие болмау мәселесін жою, өйткені киберқауіпсіздік түптен келгенде отандық IT-саласының және электронды өнеркәсібінің даму деңгейіне байланысты» қажеттілігі көрсетілген.

Осыған байланысты отандық криптографиялық құралдар құру бойынша ғылыми зерттеу жұмыстарын жүргізу еліміз үшін **өзекті** болып табылады.

Бұл, ең алдымен, ғылыми-техникалық прогресстің үнемі өсіп келе жатқан қарқынымен байланысты, бұл компьютерлік технологиялардың жетілдірілуіне алып келеді. Олардың пайда болуы қауіпсіздіктің жаңа мәселелерін көтеріп қана қоймай, сонымен қатар шешілген мәселелерді жаңа тұрғыда ұсынады, ал ақпаратты қорғау проблемасын шешудің күрделілігіне төмендегілер ықпал етеді:

- компьютерлік технологияны қолдану арқылы жинақталатын, сақталатын және жіберілетін ақпарат көлемінің ұлғаюы;
- компьютерлік жүйелердің ресурстарына қол жетімділігі бар пайдаланушылар шеңберін кеңейту;
- компьютерлік жүйенің техникалық құралдарының жұмыс режимдерінің күрделенуі;
- деректерді өңдеудің автоматтандырылған жүйелеріндегі техникалық құралдар мен байланыстар санының көбеюі;
- жаңа инфокоммуникациялық технологиялардың кеңінен қолданылуы.

Рұқсат етілмеген қол жетімділіктің салдарын азайту үшін қауіпсіздік жүйесін құру қажет. Мұндай жүйені құрудың мақсаты қасақана немесе кездейсоқ деструктивті әсердің салдарының нәтижесінде ақпарат жойылуы, модификациясы немесе жылыстауы мүмкін. Бұл жағдайда тиімді қауіпсіздік жүйесі төмендегілерді қамтамасыз етуі керек.

- барлық ақпараттың немесе оның маңызды бөлігінің құпиялылығы;
- ақпараттың сенімділігі (толықтығы, нақтылығы, дұрыстығы, тұтастығы, түпнұсқалығы), кез-келген уақытта жүйе компоненттерінің жұмыс қабілеттілігі;
- пайдаланушылардың өздеріне қажет ақпараттық және жүйелік ресурстарға уақытылы қол жетімділігі;
- ақпараттық қатынастардың белгіленген ережелерін бұзғаны үшін жауапкершілікті саралау;
- ақпаратты басқару, өңдеу және алмасу процестерін үнемі бақылау.

Қорғау объектісіне байланысты қауіпсіздік жүйесінің сипатталған қасиеттерінің арасында басымдықтардың әр түрлі орналасуы мүмкін екенін атап өткен жөн. Осылайша, мемлекеттік құпияларды қорғау жағдайында ақпараттың құпиялылығына баса назар аударылады. Бұл мақсаты қауіптің ықтималдығын азайту арқылы немесе қауіпті іске асырудың салдарын азайту болып табылатын қарсы қауіп-қатерлерді анықтайды. Осы шаралар бірлесіп қауіпсіздік саясатын қалыптастырады. Көптеген шетелдік және отандық ғалымдардың жүргізген зертеулері көрсеткендей, ұйымдастырушылық, әдістемелік және техникалық шаралар арасында ақпаратты криптографиялық қорғау әдістері ерекше орын алады.

Заманауи криптографиялық әдістер, оның ішінде итеративті блоктық шифрлар жылдамдығы жоғары ақпарат тарату желілерінде қауіпсіз ақпарат

алмасуды қамтамасыз ететін, сұранысқа ие құралдардың бірі болып табылады. Ақпараттық технологияларды кеңінен қолдану және есептеу қуатының қарқынды дамуы белгілі шифрлардың криптоталдауына қауіп тудырады.

Мәліметтерді криптографиялық қорғау құралдарын құруға бағытталған зерттеулер көбінесе мемлекеттік құпияларға байланысты, сондықтан шетелдік дайын шешімдерді қолдану қауіпсіз емес. Отандық ақпаратты криптографиялық қорғау құралдарын құру, оның ішінде шифрлау алгоритмдерін құру бойынша зерттеулер жүргізу өзекті және қажетті болып табылады.

Диссертациялық жұмыстың мақсаты - позициялық емес санау жүйесінің (ПЕСЖ) мүмкіндіктерін қолдану арқылы ақпаратты шифрлау алгоритмін құру, құрылған алгоритмнің криптоберіктілігін талдау, алгоритмді бағдарламалық жүзеге асыру болып табылады.

Зерттеу мақсатына жету үшін келесі міндеттер қойылды:

- Ақпаратты криптографиялық қорғау әдістеріне шолу және талдау;
- Ақпаратты криптографиялық қорғау жүйелеріне қойылатын талаптар мен өнімділік критерийлерін талдау;
- Позициялық емес полиномды санау жүйесі негізінде симметриялық блокты шифрлау алгоритмін құру;
- Құрылған симметриялық блоктық шифрлау алгоритмін бағдарламалық жүзеге асыру;
- Құрылған симметриялық блоктық шифрлау алгоритмінің криптоберіктілігін зерттеу.

Зерттеудің нысаны - криптографиялық қорғау алгоримдері және оларға талдау жүргізу әдістері.

Зерттеудің пәні - позициялық емес полиномды санау жүйесі негізінде құрылған шифрлау және раундық кілттерді түзу алгоритмдері.

Зерттеу әдістері - модулді арифметика, позициялық емес полиномды санау жүйесі, статистикалық тестер, биттік шашырау критерийлері, криптоталдау әдістері.

Зерттеудің ғылыми жаңалығы. Ақпараттарды қорғау мәселесі әліде шешімін таппаған күрделі проблемалардың бірі. Осы проблемаларды назарға алып, шешу алгоритмі ұсынылып, біршама жаңа жетістіктерге қол жеткізіп, ол ғылыми нәтижелер жоғары рейтингті журналдарда жарияланды. Сол ғылыми нәтижелер жаңалығы диссертациялық жұмыста негізге алынды. Атап айтар болсақ:

- ЕМ түрлендіру әдісін қолдану арқылы жаңа симметриялы блоктық шифрлау алгоритмі құрылды;
- Криптоталдау талаптарын қанағаттандыратын S-блок алмастыру кестесі құрылды;
- Раундттық кілттерді жасау алгоритмі құрылды;
- Шифрлау жылдамдығын арттыру мақсатында таңдап алған жұмыс негіздерінің индекс кестесі құрылды.

Жұмыстың теориялық және практикалық маңызы. Диссертациялық зерттеуде алынған нәтижелер телекоммуникациялық және ақпараттық жүйелер мен желілердегі, электрондық құжат айналым жүйелеріндегі ақпараттарды сонымен қатар отандық ақпараттық-коммуникациялық технологиялардың бағдарламалық өнімдерін, мемлекеттік және жеке тұлғаның рұқсат етілмеген құпия мәліметтерін бөгде адамдардың ұрлауы, өзгертуінен қорғау үшін қолдануға болады. Сонымен қатар жоғарға оқу орындарында оқу үрдістерінде пайдалануға, сондай-ақ жаңа ақпаратты криптографиялық қорғау жүйелері әзірленуде қолдануға болады.

Қорғауға шығарылған негізгі тұжырым. Қазіргі заманауи симметриялық блокты шифрлеу алгоритмдерінің негізгі талаптарына сай келетін ақпараттарды қорғау ЕМ түрлендіру әдісін қолдану арқылы жаңа симметриялы блоктық шифрлау алгоритмі жасалынды.

Сонымен қатар алгоритмге қолданылған жаңа S-блок алмастыру кестесін алу әдістері ұсылып алынған S-блокқа сызықты және дифференциалды криптоталдау жүргізілді және нәтижелері белгілі алгоритмдермен салыстырылды. Алгоритмнің шифрлау жылдамдығын арттыру мақсатында позициялық емес полиномды санау жүйесі және таңдап алған жұмыс негіздерінің индекс кестесі қолданылды.

Қорғауға ұсынылатын нәтижелер. Жаңа блокты шифрлау алгоритмі құрылды. Алгоритмнің криптобериктілін анықтау мақсатында бірнеше криптоталдау әдістері арқылы талдаулар жүргізіліп нәтижелері ұсынылды.

Зерттеу нәтижелерін жүзеге асыру. Диссертатциялық жұмысты зерттеу кезеңінде алынған нәтижелер «Ақпараттық және есептеуіш технологиялар институты», «Ақпараттық қәуіпсіздік зертханасын»-да тексеріліп, 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.

Диссертация нәтижелерінің апробациясы. Зерттеу жұмысының басты нәтижелері төмендегі конференцияларда, семинарларда баяндалды және талқыланды:

– «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе" атты XLI Халықаралық ғылыми-практикалық конференция материалдары (3-4 сәуір, 2017, Алматы, Қазақстан);

– Ақпараттық және есептеуіш технологиялар институтының «Информатика және есептеу технологияларының қазіргі заманғы мәселелері» ғылыми конференция материалдары (29-30 маусым, 2017, Алматы, Қазақстан);

– II Халықаралық «Информатика және қолданбалы математика» ғылыми-практикалық конференциясы (27-30 қыркүйек, 2017 ж., Алматы, Қазақстан);

– III Халықаралық «Информатика және қолданбалы математика» ғылыми-практикалық конференциясы (26-29 қыркүйек, 2018 ж., Алматы, Қазақстан);

– «XXI ғасыр ғылымы: жаңа көзқарас»: студенттердің, аспиранттардың және жас ғалымдардың XXIII халықаралық ғылыми-практикалық конференцияның материалдары (22-23 мамыр, 2019 ж., г. Санкт-Петербург, Россия);

– IV Халықаралық «Информатика және қолданбалы математика» ғылыми-практикалық конференциясы (25-29 қыркүйек, 2019 ж., Алматы, Қазақстан);

– «Қазақстандағы ақпараттық қауіпсіздігінің өзекті мәселелері АҚӨМ-2020» халықаралық ғылыми-практикалық конференциясы (15 қаңтар, 2020 ж., Алматы, Қазақстан);

– «Ақпараттық және есептеуіш технологиялар» институты «Информатика, математика және басқарудың өзекті мәселелері» атты ғылыми-практикалық семинарлары (2017-2020, Алматы, Қазақстан);

– Әл–Фараби атындағы Қазақ ұлттық университеті «Ақпараттық технологиялар» факультеті ғылыми семинарлары (2017-2020, Алматы, Қазақстан).

Жарияланымдар. Диссертацияның негізгі нәтижелері бойынша 14 мақала жарияланды және 1 авторлық куәлік алынды. Оның ішінде 1 мақала халықаралық рецензияланатын мерзімді басылымдарда, 6 мақала ҚР БҒМ-нің Білім және ғылым саласы бойынша бақылау комитеті ұсынған ғылыми баспаларда, 7 мақала Қазақстан мен шетелдердегі халықаралық ғылыми конференциялар жинақтарында жарияланды. Диссертациялық жұмыс бойынша шыққан мақалалар пайдаланылған әдебиеттер тізімінде келтірілді. Бағдарламалық кешенге алынған авторлық құқық куәлігі қосымшада берілді.

Ғылыми басылымдары:

1. Хомпыш А. Позициялық емес санау жүйесін қолданылуы, «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе" атты XLI Халықаралық ғылыми-практикалық конференцияның материалдары. – Алматы, 2017. – 64-66 б.

2. Капалова Н.А., Хомпыш А. Позициялық емес санау жүйесін қолданып, Эль-Гамаль шифрлау алгоритмінің модификациясын құру, Қ.И. Сәтбаева атындағы Қазақ Ұлттық техникалық зерттеу университетінің, Хабаршысы – Алматы, 2017. – №4 (122). – 506-510 б.

3. Хомпыш А. Эль-Гамаль шифрлау алгоритмінің мобильдік қосымшасын құру, «Есептеуіш технологиялар және информатиканың заманауи мәселелері» атты ғылыми конференция материалдары. – Алматы, 2017. – 281-284 б.

4. Хомпыш А. Позициялық емес санау жүйесін негізінде құрылған Эль-Гамаль шифрлау алгоритмін мәліметтер алмасу желісінде пайдалану, II Халықаралық «Информатика және қолданбалы математика» ғылыми конференция материалдары. – Алматы, 2017. – 157-161 б.

5. Капалова Н.А, Хомпыш А., Алгазы К.Т. Модуль бойынша дәрежеге шығару негізінде ақпаратты криптографиялық қорғау алгоритмінің модификациясы, М.Тынышбаев атындағы Қазақ көлік және

коммуникациялар академиясының, Хабаршысы – Алматы, 2018. – №4 (107). – 247-253б.

6. Хомпыш А. Модуль бойынша дәрежеге шығару операциясы негізінде ақпаратты криптографиялық қорғау алгоритмін бағдарламалық жүзеге асыру, III Халықаралық «Информатика және қолданбалы математика» ғылыми конференция материалдары. – Алматы, 2018. – 167-171 б.

7. Хомпыш А. Криптостойкости S-блоков в алгоритме шифрования на основе ЕМ, «Наука XXI века: новый подход»: Материалы XXIII молодёжной международной научно-практической конференции студентов, аспирантов и молодых учёных. – г. Санкт-Петербург, 2019. – С. 15-19.

8. Дюсенбаев Д.С., Сақан Қ.С., Хомпыш А., Алгазы К. «MODNPSS14» шифрлау алгоритміне криптографиялық талдау, М.Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясының, Хабаршысы – Алматы, 2019. – №3 (110). – 235-243б.

9. Бияшев Р.Г., Капалова Н.А., Алғазы К.Т., Дюсенбаев Д.С., Хомпыш А. Криптоанализ генератора псевдослучайных последовательностей и ее модификация, Вестник Казахского национального исследовательского технического университета имени К.И. Сатпаева. – Алматы, 2019. – №3 (133). – с.179-185.

10. Хомпыш А., Капалова Н.А., Алгазы К. ЕМ түрлендіру әдісі негізінде жасалған блокты шифрлеу алгоритміне жүргізілген бағалау тесттері, IV Халықаралық "Информатика және қолданбалы математика" ғылыми конференциясы. – Казахстан, Алматы – 2019. – 2. – 580-587 б.

11. Бияшев Р.Г., Алгазы К., Хомпыш А. Исследование разработанных алгоритмов по критерию «лавинного эффекта», Материалы международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане АПИБК-2020». Алматы – 2020. – с.107-119.

12. Бияшев Р.Г., Смоларш А., Алгазы К.Т., Хомпыш А. Encryption algorithm ‘’Qamal NPNS’’ based on a nonpositional polynomial notation, Journal of Mathematics, Mechanics and Computer Science, «Хабаршы» ҚазҰУ – Алматы, 2020. – №1 (105). – 198-207 б.

13. Kapalova N.A., Khompysh A., Müslüm A., Algazy K. A block encryption algorithm based on exponentiation transform, Cogent engineering (2020), 7:1788292, ISSN 2331-1916, V. 7. – P. 1-12

14. Хомпыш А., Капалова Н.А., Алгазы К. Исследование разработанного алгоритма на основе преобразования ЕМ по критерию «лавинного эффекта», М.Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясының, Хабаршысы – Алматы, 2020. – №3 (114). – 284-292б.

15. Хомпыш А., Капалова Н.А. Программа шифрования файлов «CryptoEM v1.0.1», ЭЕМ-ге арналған бағдарламаға алынған авторлық құқық куәлігі, №5450, 24 қыркүйек 2019 ж.

Диссертация құрылымы және көлемі. Диссертациялық жұмыс құрылымы кіріспеден, 3 бөлімнен, қорытындыдан, пайдаланылған әдебиеттер тізімінен және 4 қосымшадан тұрады.

Кіріспеде қазіргі кездегі пайдаланушылардан рұқсат етілмеген ақпараттарды криптографиялық қорғаудың заманауи блоктық алгоритмдерге қойылатын талаптарға сай келетін алгоритмдерін құру мәселесінің өзектілігін анықтайды, жұмыстың мақсатын сипайтайды, ғылыми мақсатына жету үшін қойылатын міндеттерді белгілейді, зерттеу нысаны мен пәнін, негізгі қорғауға шығарылатын тұжырым, қорғауға ұсынылған диссертациялық жұмыстың жаңалығы, сынақтан өткізу және оның нәтижелері көрсетілген.

Бірінші бөлімде Диссертациялық жұмыстың өзектілігінде көрсетілген мәселелерді шешудің ең тиімді әдістерінің бірі криптографиялық әдістер екендігін ескерсек, онда бұл бөлімде криптографиялық әдістері туралы негізгі түсініктер, терминдер және криптографиялық түрлендірудің негізгі класстары, симметриялық блокты шифрлау алгоритмдерін құру әдістерінің негізгі кезеңдері, блокты шифрлау алгоритмне қойылатын талаптар қарастырылды.

Екінші бөлімде Симметриялық блокты шифрлау алгоритмдерінің негізгі талаптарын ескере отырып жаңа блокты шифрлау алгоритмі құрылып, ұсынылып отырған алгоритмде қолданылған позициялық емес полиномды санау жүйесінің құру жолдары, алгоритмнің негізгі параметрлері, алгоритмнің шифрлау және шифрды ашу сұлбасы, сонымен қатар алгоритмге қолданылған ЕМ түрлендіру әдісі, S-блок алмастыру кестесін алу әдісі, таңдап алған жұмыс негіздерінің индекс кестесін алу және дәрежені жылдам есептеу процессі, раундттық кілттерді жасау алгоритмі сипатталды.

Үшінші бөлімде диссертациялық жұмыста ұсынылған жаңа блокты шифрлау алгоритмінің бағдарламалық кешені құрылып сипатталды. Алгоритмнің криптоберіктілін тексеру үшін шифрмәтіннің статистикалық қәуіпсіздігі бағалау және графикалық тесттер арқылы тексеріліп нәтижелері ұсынылды. Сонымен қатар алгоритмнің биттік шашырау критериилері арқылы зерттеу, S-блоққа сызықты және дифференциалды криптоталдау, алгоритмнің барлық түрлендіру процесіндегі дифференциалды талдау нәтижелері сипатталған.

Қорытындыда жұмыстың негізгі қорытындылары мен нәтижелері тұжырымдалды.