

6D100200 – «Ақпараттық қауіпсіздік жүйелері»
мамандығының PhD докторанты
Усатова Ольга Александрованың
«Ақпараттық-коммуникациялық жүйелердің қолданушыларын
аутентификациялау алгоритмін әзірлеу және зерттеу»
тақырыбындағы диссертациялық жұмысына

АНДАТПА

Қазақстан Республикасы тәуелсіздік алғаннан бері оның тұңғыш президенті Нұрсұлтан Әбішұлы Назарбаев бірнеше рет Қазақстан Республикасындағы азаматтардың мүдделерін қорғау қажеттілігіне назар аударды. Осылайша, Елбасының 1997 жылғы 10 қазандағы Қазақстан халқына «Қазақстан – 2030. Барлық Қазақстандықтардың өсіп-өркендеуі, қауіпсіздігі және әл-ауқатының артуы» жолдауында мемлекеттік қауіпсіздік ұзақ мерзімді басымдық ретінде белгіленді, мұнда ақпараттық қауіпсіздік маңызды бағыттардың бірі болып табылады.

Біздің республикамызда ақпараттық қауіпсіздікті қамтамасыз ету процестерінің кешенді механизмі ақпарат алу саласында оны Қазақстан Республикасының (ҚР) конституциялық құқықтары, егемендігі мен аумақтық тұтастығын қорғау үшін, сондай-ақ, қаржылық, әлеуметтік тұрақтылық, тиімді халықаралық серіктестік қалыптастыруда ақпараттық қауіпсіздікті қамтамасыз етуін қолдана алатын адамның, азаматтың конституциялық құқықтары мен бостандықтарын қамтамасыз ете алатын ұйымдастырушылық, әлеуметтік, техникалық және бағдарламалық тәсілдерді қамтиды.

2012 жылғы 6 қаңтарда қабылданған «Қазақстан Республикасының ұлттық қауіпсіздігі туралы» заңда мемлекеттің және тұтастай алғанда азаматтардың ақпараттық қауіпсіздігіне әсер ететін мемлекеттің ұстанымынан нақты анықтамалар беретін қажетті баптар бар.

Қазақстан Республикасында заңнамалық деңгейде ақпараттық қауіпсіздікті, электрондық құжат айналымы, автоматтандырылған ақпараттық жүйелер, ресурстар, АКТ, сондай-ақ маңызды объектілерді қамтамасыз етудің ұлттық тұжырымдамасы қалыптасуда және бекітілуде.

Телекоммуникациялық байланыс желілерін салу және пайдалану кезінде Қазақстан Республикасының байланыс саласындағы ұлттық қауіпсіздікті сақтау туралы талаптарын ескеру қажет. Бұған 2017 жылғы 27 желтоқсандағы «Қазақстан Республикасы мемлекеттік органдарының өкілеттіктері туралы» мақаланың соңғы заңды түзетілуі дәлел бола алады.

Телекоммуникациялық байланыс желілерін салу және пайдалану кезінде Қазақстан Республикасының байланыс саласындағы ұлттық қауіпсіздікті сақтау туралы талаптарын ескеру қажет. Бұған 2017 жылғы 27 желтоқсандағы «Қазақстан Республикасы мемлекеттік органдарының өкілеттіктері туралы» бапқа енгізілген соңғы түзету дәлел бола алады.

2013 жылғы 21 мамырда Қазақстан Республикасының № 94-V «Дербес деректер және оларды қорғау туралы» заңы қабылданды (2017 жылғы 28

желтоқсанда толықтырылған), ол жеке мәліметтерді жинауға, өңдеуге және қорғауға байланысты қатынастарды реттейді. «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы № 418-V (01.01.2020 ж. толықтырылған) ҚР заңы және «Электрондық құжат және электрондық цифрлық қолтаңба туралы» 2003 жылғы 7 қаңтардағы № 370-II (25.11.2019 ж. толықтырылған) ҚР заңы маңызды болып табылады.

Ақпараттық-телекоммуникациялық технологияларды дамыту Интернет желісінде жаңа мүмкіндіктерді пайдалануға мүмкіндік береді. Елдің кез келген нүктесінен тауарларды қашықтықтан сатып алу, жұмыстардың жай-күйі мен орындалуын бақылау мүмкіндігі пайда болды. Қазіргі уақытта электрондық цифрлық қолтаңбаның және мемлекеттік қызметтердің ақпараттық порталының арқасында үйден шықпай-ақ кез келген анықтаманы ресімдеуге мүмкіндік бар.

Қазақстан Республикасында 2017 жылғы 12 желтоқсанда Үкіметтің №827 қаулысымен «Цифрлық Қазақстан» мемлекеттік бағдарламасы бекітілді. Бұл бағдарламада негізгі аспект ел экономикасын дамыту және инфокоммуникациялық технологияларды жетілдіру мен дамытуды жеделдетуге және цифрлық экономиканы құруға негізделген халықтың тыныс-тіршілігін арттыру болып табылады. Ақпараттық-коммуникациялық технологиялар саласында ақпараттық қауіпсіздікті қамтамасыз етуге және елімізде автоматтандырылған ақпараттық жүйелердің киберқауіпсіздігін шоғырландыруға басты назар аударылды.

Технологиялық прогрестің және ақпараттандырудың жалпы деңгейінің дамуымен қатар жаңа қауіп-қатерлер де пайда болады. Киберқылмыс зиянкестерге шабуыл жасау мақсатынан мыңдаған шақырым қашықтықта бола отырып, құқыққа қарсы және заңсыз әрекеттер жасауға мүмкіндік береді. "Қазақстанның Үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік" атты Қазақстан халқына Жолдауында Қазақстан Республикасының тұңғыш президенті киберқылмыспен күрес аса өзектілікке ие екенін атап өтті.

Осыған байланысты Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысымен киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») әзірленді және бекітілді, онда электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау, ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттары анықталды.

Ақпараттық технологиялар біздің өміріміздің ажырамас бөлігіне айналды, осыған байланысты адамның тіршілік әрекетінің көптеген процестерін автоматтандыру жүзеге асырылуда. Ақпараттың көп бөлігі қорғалуы керек ақпараттық жүйелерде сақталады. Ақпараттық жүйелерге шабуылдарда зиянкестер бағдарламаларды жазу мен әкімшілендірудегі қателіктерді, сондай-ақ қажетті ақпаратты алу үшін әлеуметтік психология әдістерін қолданады. Ресурстарды әзірлеушілер қолдаланушылардың жұмыс істеуі керек деректерін қорғауға және ақпараттың таралып кету мүмкіндігін болдырмауға міндетті. ҚР негізгі проблемаларының бірі отандық ақпараттық қауіпсіздік индустриясының, атап айтқанда криптография құралдарын әзірлеудегі әлсіз дамуы болып

табылады. Қазақстанда қазіргі уақытта қолданыстағы электрондық деректерді қорғау жүйелерінде шетелдік криптографиялық алгоритмдер мен стандарттар пайдаланылады. Деректер қауіпсіздігіне қатысты зерттеулер мемлекеттік құпиялармен тікелей біріктірілген және шетелдік дайын шешімдерді қолдану өте қауіпті, осыған байланысты ақпараттың қауіпсіздігі үшін жеке ресурстарды қалыптастыру қажет.

ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институтында (ҚР БҒМ ҒК АЕТИ) ақпаратты криптографиялық қорғау және қолжетімділікті шектеу бойынша ғылыми-зерттеу жұмыстары (ҒЗЖ) жүргізіледі. Бұл ҒЗЖ ақпараттық қауіпсіздік зертханасының қызметкерлері (зертхана меңгерушісі, т.ғ.д., проф. Бияшев Р.Г., ҚР ҰҒА академигі Калимолдаев М.Н., т.ғ.д., асс. профессор Нысанбаева С.Е., ЖҒҚ, т.ғ.к. Капалова Н.А., PhD Бегимбаева Е. Е. Е., ғылыми қызметкерлер О.А. Рог, Д.С. Дюсембаев, К.Е. Алғазы, А.В. Варенников және т.б.) айналысады.

Осы қызметті жүзеге асыру үшін ҚР БҒМ ҒК АЕТИ-на ҚР Ұлттық қауіпсіздік комитетінің 2017 жылдың 03 шілдесінде №549 мемлекеттік лицензиясы берілді.

Ақпараттық жүйелерді бөгде араласудан қорғаудың негізгі құралдарының бірі сәйкестендіру және аутентификациялау болып табылады, өйткені ақпаратты қорғау тетіктері аталған субъектілер мен объектілермен жұмыс істеуге есептелген. Аутентификация және пайдаланушыны сәйкестендіру шынайылықты тану мен тексерудің өзара тәуелді әрекеттері болып табылады.

Ақпараттық жүйені пайдаланушыны аутентификациялаудың негізгі мақсаты қауіпсіздік қатерін азайту, атап айтқанда ақпараттың құпиялылығы мен тұтастығын бұзу болып табылады. Рұқсатсыз қол жеткізу жүйенің жұмыс істеу қабілеттілігіне тікелей қауіп төндіретін бұзушылықтардың ең көп таралған түрлерінің бірі.

Аутентификация әлеуметтік желілерге, электрондық поштаға, интернет дүкендерге, интернет-банкінгке, төлем жүйелеріне және т. б. қол жеткізу үшін қолданылады. Пайдаланушының аутентификациясы келесі түрлер бойынша жіктеледі:

– құпия сөз негізіндегі аутентификация: ол бір реттік және көп реттік құпия сөздер бойынша жүргізіледі. Бірнеше рет қолданылатын құпия сөзді пайдаланушы анықтайды, ал жүйе оны мәліметтер қорында сақтайды. Ол әрбір сессия үшін бірдей. Оларға PIN-кодтар, сөздер, сандар, графикалық кілттер жатады. Бір реттік парольдер әрбір сессия үшін әр түрлі;

– бірнеше әдістерді пайдалана отырып құрамдастырылған аутентификация, мысалы, құпия сөз және криптографиялық сертификаттар. Ол ақпаратты оқу үшін арнайы құрылғыны қажет етеді;

– биометриялық аутентификация: ол жеке ақпараттың жоғалуын немесе ұрлануын болдырмайды. Тексеру пайдаланушының физиологиялық сипаттамалары бойынша өтеді, мысалы, саусақ ізі, көз торы, бетті тану және дауыс тембрі;

Құпия сөзді аутентификацияны пайдалану қазіргі уақытта қолданудың қарапайымдылығына байланысты қол жетімді және кең тараған болып

табылады. Бұл қорғаныс әдісі ақпаратты қорғау тұжырымдамасының беріктігін арттыруға әкеледі.

Ақпаратты қорғаудың тиімді әдістерінің бірі - жүйеге кірудің екі факторлы аутентификациясы. Ол қорғау жүйесіне аккаунтты байланыстыру арқылы деректерді екі есе қорғауды көздейді. Байланыстырғаннан кейін пайдаланушы деректерді верификациялау үшін осы жүйемен өзара әрекеттесуі қажет.

Екінші факторға негізделген ақпараттық қауіпсіздік, қол жетімділікті басқару және аутентификация мәселелерімен шетелдік ғалымдар Эдна Элизабет, С. Нивета, Фасех Садат Бабамир, Мурвет Кирчи, Юи, Джингшахе, Нафеи Чжу, Фанбо Цай, Мұхаммед Салман Патан және т.б. айналысты. Мәліметтер қорында сақталатын ақпаратты және ақпаратты өңдеуге, беруге арналған аппараттық және бағдарламалық қамтамасыздандыруды қорғаудың маңызы зор. Бұл бағыттың дамуына Мещеряков Р.В., Исхаков А.Ю., Полтавцева М.А. және т.б. шетелдік ғалымдар елеулі үлес қосты.

Жоғарыда айтылғандарға байланысты, екінші фактор негізінде ақпараттық-коммуникациялық жүйелерді пайдаланушылардың аутентификация алгоритмін әзірлеу және зерттеу бойынша берілген диссертациялық жұмыстың тақырыбы өзекті болып табылады. Осы диссертацияда екінші фактор ретінде бір реттік пароль болып табылады.

Зерттеу тақырыбының өзектілігі:

– электрондық ақпараттық ресурстарды, телекоммуникация жүйелері мен желілерін қорғау, ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты дамытуға бағытталған Қазақстан Республикасы Үкіметінің мемлекеттік бағдарламасында және киберқауіпсіздік тұжырымдамасында («Қазақстанның киберқалқаны») қойылған міндеттерді іске асыру;

– ақпараттық қауіпсіздікті қамтамасыз етудің отандық Қазақстандық жүйелерін әзірлеу;

– ақпаратты қорғау жүйелерінің сенімділігін арттыру мақсатында құпия сөзді екі факторлы аутентификация саясатын қолдану.

Диссертациялық жұмыстың мақсаты: ақпараттық-коммуникациялық жүйелерде ақпаратты қорғауды қамтамасыз ету үшін екі факторлы аутентификация алгоритмін әзірлеу, зерттеу және жүзеге асыру

Диссертациялық зерттеудің мақсаттарын жүзеге асыратын зерттеулер:

1. Ақпараттық-коммуникациялық жүйелердегі қолданыстағы ақпаратты қорғау жүйелеріне және көп факторлы аутентификация алгоритмдеріне шолу және талдау жүргізу.

2. Бір реттік құпия сөзді қолдана отырып, ақпараттық және коммуникациялық жүйелердегі пайдаланушыларды аутентификациялау алгоритмін құру.

3. Ақпараттық-коммуникациялық жүйелерде ақпараттың тұтастығын және қорғалуын қамтамасыз ету үшін ақпараттық жүйені құру.

Зерттеу объектісі: екінші фактор негізінде пайдаланушыны аутентификациялау кезінде рұқсатсыз кіруден ақпаратты қорғау жүйесі.

Зерттеу пәні ақпараттық-коммуникациялық жүйелерді пайдаланушылар арасындағы ақпараттық өзара әрекеттесу және олардың бір реттік сандық құпия сөзді қолдана отырып аутентификациялау процестері болып табылады.

Ғылыми жаңашылдықтар және жұмыс барысында алынған нәтижелер:

– бір реттік құпия сөзді есептеу кезінде функциялардың масштабын қиындату арқылы тригонометриялық функцияларды генерациялауға негізделген пайдаланушының екі факторлы аутентификациялау алгоритмі жасалды. Масштаптау тригонометриялық функцияның матрицалық көрінісі арқылы жүзеге асырылады және ағымдағы уақыт, құпия жол, логин және алғашқы аутентификация коды бойынша тригонометриялық функциямен жасалатын координаттар мен параметрлерді есептеу үшін хэш-функцияларды пайдаланумен орындалады;

– екінші фактордың негізінде пайдаланушының екі факторлы аутентификация процесінің моделі әзірленді, ол ашық және әрбір жеке жүйе үшін екінші аутентификация кодын алу функцияларының жиынтығын генерациялай алады;

– мобильді құрылғыны пайдалану арқылы жабық желіде пайдалану және енгізу үшін екі факторлы аутентификацияны бағдарламалық іске асырудың ақпараттық жүйесінің схемасы ұсынылды.

Зерттеушінің жеке үлесі. Екінші фактор негізінде ақпараттық жүйеде пайдаланушыны аутентификациялау алгоритмі әзірленді. Ұсынылған модельдер мен алгоритмдерге сандық зерттеулер мен эксперименттік бағалау жүргізілді. Аутентификатордың компьютерлік бағдарламасын және ұялы телефонды пайдалана отырып, бір реттік қолданылатын құпия сөзді генерациялау кезінде ұсынылған пайдаланушының аутентификациялау жүйесінің бағдарламасы жүзеге асырылды және аутентификацияның клиент-серверлік жүйесінің архитектурасы әзірленді.

Диссертация тақырыбының ғылыми - зерттеу жұмыстарының жоспарларлаымен байланысы. Ұсынылған нәтижелер ҚР БҒМ ҒК АЕТИ-ның келесі жобаларын жүзеге асыру барысында алынды (қаржыландыру көзі: ҚР БҒМ ҒК):

– 2018-2019 жж. «Инфокоммуникациялық жүйелер мен жалпы мақсаттағы желілерде ақпаратты беру және сақтау кезінде ақпаратты криптографиялық қорғау үшін бағдарламалық және бағдарламалық-аппараттық құралдарды әзірлеу» бағдарламалық-нысаналы қаржыландыру (БНҚ) ҚР БҒМ ҒК;

– 2020 ж. «Өзара іс-қимылдың Қазақстандық ақпараттық қорғалған трансшекаралық сегментін әзірлеу» гранттық қаржыландыруы (ГК) ҚР БҒМ ҒК.

Басылымдар. Диссертация тақырыбы бойынша жүргізілген зерттеулердің негізгі нәтижелері 15 басылымда ұсынылған, оның ішінде 5 - ҚР БҒМ ҒК ұсынған ғылыми басылымдарда, 2 - Scopus және Web of Science мәліметтер базасына кіретін Халықаралық ғылыми басылымдарда, 8 - халықаралық ғылыми-практикалық конференция материалдарында.

Жұмыстың көлемі мен құрылымы. Жұмыстың жалпы көлемі - 123 бет.

Диссертация кіріспеден, 3 бөлімнен, қорытындыдан, 104 атаудан, 4 қосымшадан, 37 сурет пен 5 кестеден тұрады.

Кіріспе бөлімде жұмыстың өзектілігі анықталады, зерттелетін тақырыпқа байланысты мәселелер көрсетілді. Зерттеудің мақсаты, объектісі, пәні мен міндеттері тұжырымдалған. Зерттеу нәтижелері сипатталған, олардың ғылыми жаңашылдығы мен практикалық маңыздылығы көрсетілген. Диссертация нәтижелерін сынақтан өткізу туралы мәліметтер келтірілген.

Бірінші бөлімде екі факторлы аутентификация негізінде ақпараттық жүйелерді қорғаудың танымал әдістері мен құралдарын зерттеуге арналған. Пайдаланушы аутентификациясы кезінде мәліметтер базасында ақпараттық қауіпсіздікті құру принциптері сипатталған.

Ақпараттық жүйелерде қолданылатын екі факторлы аутентификациялаудың кең тараған әдістерінің жіктелуі ұсынылған, осы әдістердің кемшіліктері мен артықшылықтары қарастырылған.

Бір реттік кодты қолдану арқылы аутентификация алгоритмдері мен хаттамалары қарастырылған. HOTP (HMAC – Based One – Time Password Algorithm) – бір реттік қолдану арқылы қорғалған аутентификация алгоритмінің кодына негізделген SHA-1 және TOTP (Time – based One – Time Password Algorithm) қорғалған аутентификация үшін бір реттік құпия сөздерді құру алгоритмі негізі болып табылатын бір реттік парольдерді әзірлеу үшін қорғалған аутентификация. Екі факторлы аутентификация негізінде ақпаратты қорғау жүйелері мен олардың сипаттамаларына талдау жүргізілді. Ақпараттық қауіпсіздікті қамтамасыз ету саласында маманданған компаниялардың статистикалық деректері келтірілді. Кибершабуылдарға талдау жүргізілді және мәліметтер базасында сақталған ақпаратты қорғау бойынша қызметтерді ұсынатын кейбір компаниялар қарастырылды. Дайын аутентификаторлардың шешімдерін қолдану кезінде туындайтын мәселелер сипатталды.

Екінші бөлімде екі факторлы аутентификация негізінде пайдаланушыны сәйкестендіру кезінде ақпараттық жүйені қорғау моделін әзірлеу кезінде алынған нәтижелер көрсетілген. Бір реттік құпия сөзді қолдану арқылы аутентификация әдістері қарастырылған. Екінші фактор негізінде пайдаланушыны аутентификациялау үшін бір реттік кілтті генерациялау моделіне негізделген аутентификатор және ұялы телефон бағдарламасын пайдалана отырып, бір реттік қолданылатын құпия сөзді генерациялау алгоритмі әзірленді және сипатталған. Әзірленген модель екі факторлардың комбинациясын қолдануға негізделген: тұрақты және уақытша құпия сөздер.

SHA256 хеш функциясы сипатталған, ол функциялар жиынтығын генерациялау және бір реттік құпия сөзді есептеу үшін кіріс параметрі ретінде пайдаланылады. SHA256 хеш-функциясын қалыптастыру үшін пайдаланушының логині мен құпия сөзі, ағымдағы уақыт/күн және құпия жол сияқты мәліметтер ескеріледі. Екі факторлы аутентификацияның бір реттік құпия сөзін қалыптастыру үшін құрылған кездейсоқ құпия сөздердің генераторлары және тригонометриялық функциялар қарастырылған.

Үшінші бөлімде екі факторлы аутентификацияның бұрынғы алгоритмінің бағдарламалық іске асыру нәтижелері келтірілген. Өзара

әрекеттесетін 3 модульден тұратын ақпараттық жүйе құрылды: пайдаланушы, мобильді қосымша және сервер бөлігі. Осы модульдердің әрқайсысының құрылымы қарастырылды.

JavaScript бағдарламасының тілінде берілген бағдарламалық коды бар мәліметтер базасында сақталатын ақпаратты қорғауға қолдану схемасы және Base64 алгоритмі сипатталды. Желіде файл алмасуға және веб-сайт трафигін қорғауға арналған стандартты TLS (Transport Layer Security) және SSL (Secure Socket Layer) хаттамалары қарастырылды.

MongoDB МББЖ жұмысы сипатталған, онда мәліметтер сақталады және өңделеді. Алгоритмді жүзеге асыру кезінде қолданылатын объектілі-бағытталған тәсіл сипатталды.

Қосымшаның құрылымы кезең-кезеңмен сипатталған. Пайдаланушы аутентификациясы кезінде бір реттік кілт негізінде ақпараттық қауіпсіздік ақпараттық жүйесін компьютерде енгізу жүзеге асырылды және ұсынылған алгоритмнің дұрыстығы зерттелді.

Қорытындыда диссертациялық зерттеудің негізгі нәтижелері мен қорытындылары баяндалған. Зерттеу нәтижелері ҚР БҒМ ҒК АЕТИ-ның «Ақпараттық қауіпсіздік» зертханасында орындалатын жоғарыда көрсетілген 2018-2019 жылдардағы БНҚ және 2020 жылдың ГҚ жобалардың есептеріне енгізілді.

Сенімділік дәрежесі мен апробациялау нәтижелері. Зерттеудің дұрыстығы мен сенімділігі тапсырманың негізделген міндеттеріне, анализ критерийлері мен осы саладағы зерттеулердің жай-күйіне, көптеген эксперименттерге және оларды тәжірибеде сәтті жүзеге асыруға келеді. Диссертацияның нәтижелері келесі ғылыми-әдістемелік конференцияларда талқыланып, баяндалды:

1. «Төртінші өнеркәсіптік революция жағдайындағы дамудың жаңа мүмкіндіктері» атты ҚР Президенті Н. Назарбаевтың Жолдауын іске асыру шеңберінде «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе» атты ХЛІІ халықаралық ғылыми-практикалық конференцияда (ҚазККА, Қазақстан, Алматы, 2018);

2. «Қазіргі заманғы информатика және есептеу» ғылыми конференциясы (ҚР БҒМ ҒК АЕТИ, Қазақстан, Алматы, 2018);

3. «Информатика және қолданбалы математика» халықаралық ғылыми конференция (ҚР БҒМ ҒК АЕТИ, Қазақстан, Алматы, 2018);

4. Абай атындағы ҚазҰПУ-дың 90 жылдығына байланысты халықаралық ғылыми-әдістемелік конференция (Қаз НПУ, Қазақстан, Алматы, 2018);

5. International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019) (Guilin, China, 2019);

6. «Қазіргі заманғы информатика және есептеу» ғылыми конференциясы (ҚР БҒМ ҒК АЕТИ, Қазақстан, Алматы, 2019);

7. «Информатика және қолданбалы математика» халықаралық ғылыми-тәжірибелік конференция (ҚР БҒМ ҒК АЕТИ, Қазақстан, Алматы, 2019);

8. «Қазақстандағы ақпараттық қауіпсіздіктің өзекті мәселелері» халықаралық-тәжірибелік конференция (ҚР БҒМ ҒК АЕТИ, Қазақстан, Алматы,

2020).

Диссертация тақырыбы бойынша 15 мақала жарияланды және 2 авторлық куәлік алынды:

1 Нысанбаева С.Е., Усатова О. А. «Способы обеспечения безопасности информации в базах данных»//Вестник КазНИТУ им. Сатпаева. – Алматы, 2018. – № 2. – С. 66–70.

2 Нысанбаева С.Е., Усатова О.А. «Возможное применение больших данных в системе образования»// Матер. междунар. науч. практ. конф. «Инновационные технологии на транспорте: образование, наука, практика» в рамках реализации Послания Президента РК Н. Назарбаева «Новые возможности развития в условиях четвертой промышленной революции» – Алматы, 2018. – С. 95–99.

3 Нысанбаева С.Е., Усатова О.А. «Криптографическая защита в автоматизированных системах»// Науч. конф. «Современные проблемы информатики и вычислительной технологий». – Алматы, 2018. – С. 220–223.

4 Нысанбаева С.Е., Усатова О.А. «Двухфакторная аутентификация в автоматизированной системе управления»// III Междунар. науч. конф. «Информатика и прикладная математика». – Алматы, 2018. – С. 239–242.

5 Усатова О.А., Науменко В.В. «Статистические исследования инфраструктурной платформы с использованием систем защиты данных»// VIII междунар. науч.-метод. конф. посвященной 90-летию юбилею Казахского национального педагогического университета имени Абая. – Алматы, 2018. – С. 113–116.

6 O. Ussatova, S. Nyssanbayeva, W. Wojcik. «Development of an authentication model based on the second factor in an automated control system»// Вестник КБТУ. – Алматы, 2019. –Т.16. – С.115–118.

7 S. Nyssanbayeva, W. Wojcik, O. Ussatova. «Algorithm for generating temporary password based on the two-factor authentication model»// Przegląd Elektrotechniczny. – Polan, 2019. –№ 5. – P. 101–106.

8 O. Ussatova, S. Nyssanbayeva, W. Wojcik. «Two-factor authentication algorithm implementation with additional security parameter based on mobile application »// International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019). –Guilin, China, 2019. – Vol. 89. – P. 84–86.

9 O. Ussatova, S. Nyssanbayeva, W. Wojcik. « Software implementation of two-factor authentication to ensure security when accessing an information system» // Вестник КазНУ им.аль-Фараби. –Алматы,2019. – С.87–95.

10 Olga Ussatova, Saule Nyssanbayeva. «Generators of one-time two-factor authentication passwords»// Informatyka, Automatyka, Pomiaru w Gospodarcei Ochronie Środowiska. – Poland, 2019. № 2. – P. 60–64.

11 Усатова О.А., Нысанбаева С.Е. «Обеспечение защиты информационной системы с помощью двухфакторной аутентификации»// науч. конф. «Современные проблемы информатики и вычислительных технологий» – Алматы, 2019. –С. 337–343.

12 Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule. «Development of an automated system model of information protection in the cross-border exchange»// Cogent Engineering Journal. – 2020. DOI: 10.1080/ 23311916. 2020.1724597. –Р. 1–13.

13 Бегимбаева Е.Е., Усатова О.А., Бияшев Р.Г., Нысанбаева С.Е., Вуйцик В., «Разработка модулей для защиты информации в автоматизированной системе с применением разграничения доступа»// IV междунар. науч.– практ. конф. «Информатика и прикладная математика», посвященная 70–летнему юбилею профессоров Биярова Т.Н., Вальдемара Вуйцика и 60–летию профессора Амиргалиева Е.Н. – Алматы, 2019. – С. 595–602.

14 Усатова О.А., Нысанбаева С.Е. «Исследование и разработка модели защиты базы данных информационной системы»// Вестник КазНУ им.аль-Фараби, Алматы, 2019. – № 4 (104), – С.95–106.

15 Усатова О.А. «Клиент-серверная система защиты информации на основе двухфакторной аутентификации»// междунар. науч.– практ. конф. «Актуальные проблемы информационной безопасности в Казахстане». – Алматы, 2020. – С. 243–248.

16 Сертификат регистрации авторского права на алгоритм «Двухфакторная аутентификация в автоматизированной системе управления» №712144534 от 2018.10.01, компании «WORKS COPYRIGHT», это цифровая сертификация, юридически признанная во всем мире для регистрации авторских прав авторов, New York – NY–USA.

17 Авторское свидетельство о внесении сведений в государственный реестр прав на объекты, охраняемые авторским правом РК, № 4330 от 28 июня 2019г., «Система аутентификации с использованием второго фактора для контроля доступа к данным – Security Code of the 2FA».