

А.Б. Досжанова^{1*} , Д.Б. Бұғыбай² ¹Қазақстан Республикасы Бас прокуратурасы жанындағы құқық қорғау академиясы
Қосшы қ., 010078, Қазақстан Республикасы²Ш.Есенов атындағы Каспий технологиялар және инжиниринг университеті
Ақтау қ., 130000, Қазақстан Республикасы*e-mail: aitok82@mail.ru

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР АРҚЫЛЫ ТҮЛҒАНЫҢ ЖЕКЕ БАСЫН АНЫҚТАУДЫҢ ҚАЗІРГІ ЖАЙ-КҮЙІ МЕН ПЕРСПЕКТИВАЛАРЫ

Андатпа

Мақалада Қазақстанда жеке тұлғаны сәйкестендіру үшін ақпараттық-коммуникациялық технологияларды (АКТ) қолдану, сондай-ақ биометриялық деректерді құқықтық реттеу және қорғау мәселелері зерттеледі. Мақалада «Цифрлық Қазақстан» бағдарламасы аясында белсенді қолданылатын, бет-әлпетті тану және саусақ іздерін сәйкестендіру жүйелері сияқты заманауи сәйкестендіру технологиялары қарастырылады. Қазақстандағы жеке мәліметтерді қорғау және киберқауіпсіздік саласындағы құқықтық базаны талдауға және қолданыстағы заңнаманы жетілдіру қажеттілігіне ерекше назар аударылады.

Зерттеудің әдіснамалық негізіне нормативтік құқықтық актілерді, ірі қалалардағы қылмыс деңгейінің төмендеуі туралы статистикалық мәліметтерді талдау, сондай-ақ АКТ қолданудың халықаралық тәжірибесіне салыстырмалы талдау кіреді. Мақалада Астана және Алматы қалаларында биометриялық жүйелерді қолданудың нәтижелері көрсетілген, мұнда бет-әлпетті тану технологияларын енгізу нәтижесінде қылмыс деңгейінің 20-25%-ға төмендеуі байқалады. Зерттеу барысында анықталған негізгі проблемаларға биометриялық ақпаратты құқықтық қорғаудың жеткіліксіздігі және кибершабуылдарға осалдығы жатады.

Зерттеудің теориялық маңыздылығы АКТ-ның жеке тұлғаны сәйкестендіру процесіндегі рөлін дамытуда, сондай-ақ биометриялық деректерді қолданудың құқықтық және этикалық аспектілерін талдауда жатыр. Зерттеудің практикалық маңыздылығы Қазақстандағы заңнаманы жетілдіруге, жеке мәліметтерді қорғауды күшейтуге және цифрлық инфрақұрылымды дамытуға арналған ұсыныстар беруде. Мақалада биометриялық сәйкестендірудің жаңа әдістерін зерттеу және киберқауіпсіздік тетіктерін әзірлеу сияқты болашақ зерттеу бағыттары көрсетілген.

Негізгі сөздер: жеке тұлғаны сәйкестендіру, ақпараттық-коммуникациялық технологиялар, биометриялық деректер, жеке мәліметтерді қорғау, бет-әлпетті тану, киберқауіпсіздік, құқықтық реттеу.

Кіріспе

Ақпараттық-коммуникациялық технологиялардың (АКТ) дамуы өмірдің түрлі салаларына, соның ішінде жеке тұлғаны анықтау үдерістеріне айтарлықтай әсер етеді.

Жалпы АКТ дамуына жетпестен бұрын, А.И. Ракитовтың технология терминін: "...кәдімгі мағынадағы технология - бұл тиісті кеңістіктік-уақыттық интервалдарда және толық негізде белгіленген ретпен жүзеге асырылатын әртүрлі операциялар мен дағдылардың жиынтығы [1] ретінде, яғни қоғамның цифрлануы және бет-әлпетті тану, саусақ іздері және дауысты сәйкестендіру жүйелері сияқты биометриялық технологиялардың белсенді енгізілуі жағдайында жеке тұлғаны анықтау мәселелері ерекше өзектілікке ие болып отыр. Қазақстанда АКТ енгізу «Цифрлық Қазақстан» мемлекеттік бағдарламасы аясында жүзеге асырылып, оның мақсаты мемлекеттік қызметтердің тиімділігін арттыру және озық технологияларды пайдалану арқылы азаматтардың қауіпсіздігін қамтамасыз ету болып табылады.

Соған қарамастан, осы саладағы елеулі жетістіктерге қарамастан, шешуді қажет ететін бірқатар мәселелер бар. Негізгі мәселелердің бірі - жеке деректерді қорғау және киберқауіпсіздік. Жақында биометриялық ақпараттардың таралуы және сәйкестендіру жүйелеріне бағытталған кибершабуылдар оқиғалары жаңа технологиялардың әкелген қауіп-қатерлерімен қазіргі құқықтық тетіктердің әрдайым күресе алмайтынын көрсетті. Этикалық

мәселелер де биометриялық деректерді қолданудың заңдылығына қатысты пікірталастарда маңызды орын алады, бұл нақты ережелер мен стандарттарды әзірлеуді талап етеді.

Зерттеудің мақсаты - Қазақстандағы жеке тұлғаны сәйкестендіру үшін АКТ-ны қолданудың қазіргі жағдайын және перспективаларын талдау, құқықтық реттеудегі бар мәселелер мен кемшіліктерді анықтау, сондай-ақ АКТ-ны Қазақстан мен шет елдерде қолданудың сәтті мысалдарын қарастыру. Зерттеу барысында деректерді қорғаудың жалпы ережесі (GDPR) сияқты халықаралық стандарттар қарастырылып, олардың Қазақстан құқықтық жүйесіне бейімделу мүмкіндігі зерттеледі.

Зерттеу Қазақстанның тәжірибесін халықаралық тәжірибемен салыстыруға, сондай-ақ жеке тұлғаны сәйкестендіру мәселелеріне арналған заңнама мен ғылыми еңбектерді талдауға негізделген. Алдыңғы зерттеулердің кемшілігі технологиялардың жылдам дамуын және киберқауіпсіздік саласындағы өсіп келе жатқан қауіптерді ескермегендігінде, сондықтан бұл зерттеу ерекше өзекті болып отыр.

Зерттеу материалдары мен әдістері

Қазақстандағы жеке тұлғаны сәйкестендіру үдерістерін АКТ арқылы зерттеу кешенді сипатқа ие болып, бірнеше негізгі кезеңдерді қамтиды. Зерттеу нысаны ретінде бет-әлпетті тану (Face ID) және саусақ іздерін сәйкестендіру сияқты биометриялық сәйкестендіру жүйелері, сондай-ақ Қазақстанда және шет елдерде олардың енгізілуінің құқықтық және ұйымдастырушылық аспектілері таңдалды.

Зерттеу аналитикалық зерттеулерге жатады, ол салыстырмалы құқықтық талдау мен түрлі елдерде жеке тұлғаны сәйкестендіру үшін АКТ енгізу тәжірибесін зерделеуге негізделген. Негізгі назар Қазақстанның тәжірибесіне және оны Еуропалық Одақ, АҚШ және Қытай сияқты елдердегі халықаралық тәжірибемен салыстыруға аударылады.

Зерттеудің мақсатына жету үшін келесі әдістер қолданылды:

Нормативтік-құқықтық актілерді талдау: Қазақстан Республикасының жеке деректерді қорғау және биометриялық технологияларды пайдалануды құқықтық реттеу саласындағы заңнамасы зерттелді. Салыстырмалы талдау Еуропалық Одақ елдерінің нормативтік актілерімен, соның ішінде Деректерді қорғаудың жалпы регламентімен (GDPR), және АҚШ заңнамасымен жүргізілді. 2020 жылдан бері Қазақстандағы Dentons командасы өз клиенттерін Дербес деректер туралы заңнаманы жетілдіру үшін қабылданған өзгерістер мен түзетулер туралы үнемі хабардар етіп отырады. Бұл өзгерістерді талдау Қазақстанның мақсаты GDPR стандарттарына біртіндеп көшу арқылы дербес деректер туралы заңнаманы күшейту болып табылатынын айқын көрсетеді [2].

Ғылыми әдебиеттерді талдау: жеке тұлғаны сәйкестендіру, ақпараттық қауіпсіздік және құқықтық реттеу мәселелері бойынша қазақстандық және шетелдік авторлардың жарияланымдары зерттелді. Зерттеу барысында ғылыми мақалалар, монографиялар және конференция материалдары пайдаланылды.

Статистикалық деректердің контент-талдауы: Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің ашық деректері, сондай-ақ қауіпсіздікті қамтамасыз ету процесінде биометриялық технологияларды қолдану бойынша құқық қорғау органдарының статистикасы қолданылды.

Талдау әдістері АКТ-ны Қазақстанда қолданудың негізгі үрдістерін, мәселелерін және перспективаларын анықтауға бағытталған. Құқықтық реттеу жағдайын бағалау үшін Қазақстан Республикасының қолданыстағы заңдары мен нормативтік актілері, соның ішінде «Жеке деректер және оларды қорғау туралы» Заңы талданды. Техникалық тиімділікті бағалау үшін Астана және Алматы қалаларында биометриялық технологияларды енгізу және пайдалану нәтижелері туралы деректер, қылмыс деңгейінің төмендеуі туралы ресми есептерден алынған статистика пайдаланылды.

Зерттеу нәтижелері Қазақстанда жеке тұлғаны сәйкестендіру үшін АКТ-ны пайдаланудың халықаралық мысалдармен салыстырғандағы артықшылықтары мен

кемшіліктерін көрнекі түрде көрсетуге мүмкіндік берді. Деректерді өңдеу үшін сандық және сапалық талдау әдістері қолданылды, бұл АКТ енгізу мен оның қауіпсіздікке және жеке деректерді қорғауға әсері арасындағы байланыстарды анықтауға мүмкіндік берді.

Аталған зерттеуде адамдарға немесе жануарларға тәжірибелер жүргізілген жоқ, алайда зерттеу құпиялылық және жеке деректерді қорғау қағидаттарына сәйкес жүргізілді. Тек ашық ақпарат көздері пайдаланылды, жеке деректер қамтылмаған. Заңнаманы зерттеу барысында цифрландыру жағдайында азаматтардың жеке өмірін қорғау құқықтарын қорғаудың этикалық аспектілері де ескерілді.

Нәтижелер және оларды талқылау

Зерттеу нәтижелері АКТ-ны жеке тұлғаны сәйкестендіру үшін қолданудың халықаралық тәжірибесімен салыстырылады. Еуропалық Одақ, АҚШ және Қытай елдерінде биометриялық жүйелер қауіпсіздікті қамтамасыз ету және қызметтерді ұсыну үшін белсенді түрде қолданылады, бұл олардың жоғары тиімділігін растайды. Алайда, Қазақстанда осы салада қосымша талдауды талап ететін бірнеше ерекшеліктер анықталды.

1. Құқықтық реттеу. Еуропалық Одақта қолданыстағы Деректерді қорғаудың жалпы регламенті (GDPR) күшіне енгенімен, Қазақстан заңнамасы цифрлық дәуірдің сын-қатерлеріне толығымен бейімделмеген. Еуропалық Одақ биометриялық деректерді қорғаудың нақты стандарттарын белгілеген болса, Қазақстанда қатаң қорғаныс механизмдерін әзірлеу кезеңі жүріп жатыр. Бұл халықаралық тәжірибені бейімдеу және ұлттық құқықтық жүйеге үздік тәжірибелерді енгізу мүмкіндігін тудырады.

2. Техникалық және инфрақұрылымдық шектеулер. Қазақстан биометриялық жүйелерді енгізуде, әсіресе цифрлық инфрақұрылымы әлсіз дамыған өңірлерде техникалық қиындықтарға тап болып отыр. Мұндай технологиялар кеңінен қолданылып жүрген АҚШ және Қытай сияқты елдерден айырмашылығы, Қазақстан АКТ-ны кең ауқымды қолдану үшін толыққанды инфрақұрылымды құру жолында тұр. Бұл айтарлықтай инвестиция мен мамандар даярлауды қажет етеді.

3. Этикалық аспектілер. Этика және азаматтардың құпиялылық құқықтарын қорғау мәселелері де өзекті болып қалуда. Қазақстанда биометриялық ақпаратты пайдаланудың ашықтығын және азаматтарға олардың деректерін өңдеу мақсаттары мен әдістері туралы ақпарат беруді қамтамасыз ететін ережелерді енгізу қажет. Бұл аспектілерге ЕО және АҚШ елдерінде үлкен көңіл бөлінген, онда биометриялық деректерді пайдалануды реттейтін этикалық кодекстер қабылданған.

Ұсынымдар мен ұсыныстар:

1. Құқықтық реттеуді жетілдіру. Қазақстан биометриялық ақпаратты қорғауды реттейтін қатаң заңдарды әзірлеп, GDPR сияқты үздік халықаралық тәжірибелерді бейімдеуі қажет. Деректерді өңдеудің нақты ережелерін белгілеу және олардың таралуына жауапкершілікті қамтамасыз ету маңызды.

2. Цифрлық инфрақұрылымға инвестициялар. АКТ-ны сәтті енгізу үшін инфрақұрылымды дамыту, әсіресе өңірлерде, қажет. Бұл тек технологиялық шешімдермен шектелмей, киберқауіпсіздік пен АКТ саласындағы мамандарды даярлауды қамтиды.

3. Азаматтардың хабардарлығын арттыру. Азаматтарға биометриялық жүйелер мен деректерді қорғау саласындағы құқықтары туралы ақпараттандыру бағдарламаларын дамыту маңызды. Бұл осындай технологияларға деген сенімді арттырып, олардың қоғамдағы қабылдануын жақсартуға мүмкіндік береді.

Зерттеу нәтижелері Қазақстандағы жеке тұлғаны сәйкестендіру жүйесін одан әрі жетілдіру және халықаралық стандарттарды бейімдеу үшін пайдаланылуы мүмкін. Дегенмен, биометриялық технологияларды енгізу елеулі инвестицияларды және дамыған цифрлық инфрақұрылымның болуын талап етеді, бұл елдің кейбір өңірлері үшін шектеу болуы мүмкін. Осы зерттеу нәтижелеріне сүйене отырып, келесі зерттеу бағыттарын ұсынуға болады:

– киберқауіптер өсіп келе жатқан жағдайда биометриялық деректерді қорғау модельдерін әзірлеу;

– Қазақстанда көздің торын тану, дауыс арқылы сәйкестендіру сияқты жаңа биометриялық технологияларды енгізу мүмкіндіктерін талдау;

– жеке тұлғаны сәйкестендіру үшін АКТ қолданудың этикалық аспектілерін және олардың құқықтық реттелуін зерттеу.

1. Жеке тұлғаны сәйкестендірудің теориялық негіздері

Жеке тұлғаны сәйкестендіру қазіргі әлемдегі басты міндеттердің бірі болып табылады, ол АКТ дамуы жағдайында ерекше маңызға ие болуда. Жеке тұлғаны сәйкестендіру – бұл тұлғаны бірегей анықтауға мүмкіндік беретін деректер жиынтығына негізделген үдеріс. Құқықтық ғылымда бұл ұғым құқықтық реттеу, киберқауіпсіздік, дербес деректерді қорғау және адам құқықтарын сақтау мәселелерімен байланысты.

Жеке тұлғаны сәйкестендірудің заманауи тәсілдері саусақ іздері, бет-әлпетті сканерлеу (Face ID), көздің торын тексеру, дауыс және басқа да биометриялық сипаттамалар сияқты биометриялық деректерді пайдалануға негізделеді. Бұл технологиялар, өз кезегінде, сәйкестендіру үдерісінің дәлдігі мен жылдамдығын айтарлықтай арттыруға мүмкіндік беретін жасанды интеллектті, машиналық оқыту мен басқа да цифрлық технологияларды қолдануға негізделген. Бірқатар заңгерлердің еңбектерінде мұндай жеке тұлғаны сәйкестендіру әдістері құқықтық нормаларды нақтылауды және технологиялардың жылдам өзгеруіне бейімделуді талап ететін жаңа құқықтық мәселелер туғызатыны ерекше атап өтіледі.

Қазақстанда жеке тұлғаны сәйкестендіру үдерісіне АКТ-ны енгізу «Цифрлық Қазақстан» бағдарламасының дамуына байланысты өзекті болды. Қазақстан Президенті Қасым-Жомарт Тоқаевтың 2020 жылғы Қазақстан халқына Жолдауында «ақпараттық технологиялардың дамуы азаматтардың деректерін қорғау мен олардың құпиялылығын күшейтумен қатар жүруі тиіс» деп атап өткен болатын [3]. Бағдарламаның негізгі міндеттерінің бірі – «Smart City» жобалары мен мемлекеттік қызметтерге биометриялық жүйелерді енгізуді қоса алғанда, жеке тұлғаны сәйкестендіру жүйесін жетілдіруге арналған инновациялық шешімдерді пайдалану болып табылады.

2017 жылы «Зерде» ұлттық инфокоммуникациялық холдингі» АҚ Smart City тұжырымдамасын әзірледі. Аталған тұжырымдаманың негізгі мақсаты, Smart City технологияларын іске асырудың принциптері, тәсілдері, мақсаттары, басымдықтары мен міндеттері туралы негізгі көзқарастар жүйесін қамтамасыз ету болып табылады [4].

Халықаралық тәжірибе көрсеткендей, жеке тұлғаны сәйкестендіру үшін биометриялық жүйелер мен басқа да цифрлық технологияларды қолдану көптеген елдерде стандартқа айналды. Мысалы, Еуропалық Одақ пен АҚШ елдерінде биометриялық сәйкестендіру банктік салада және мемлекеттік қызметтер жүйесінде белсенді қолданылады. Қытайда бет-әлпетті тану жүйесі «Әлеуметтік несие» жобасына интеграцияланған, бұл мемлекетке азаматтардың мінез-құлық нормалары мен стандарттарын бақылауға мүмкіндік береді [5]. Дегенмен, бұл технологиялардың дамуымен қатар, құқықтық реттеу мен дербес деректерді қорғауға қатысты көптеген мәселелер туындап отыр, бұл Қазақстан үшін де өзекті.

Қазақстанда дербес деректерді қорғау туралы заңнама халықаралық стандарттарға сәйкес дамуда. «Жеке деректер және оларды қорғау туралы» Қазақстан Республикасының Заңы сияқты заңнамалық актілер биометриялық ақпаратты жинау, сақтау және пайдалану мәселелерін реттейді. Алайда, қазақстандық заңгер Б.Д. Құшқалиев атап өткендей, технологиялардың дамуы құқықтық механизмдерді одан әрі жетілдіруді және деректердің құпиялылығы мен қауіпсіздігін қамтамасыз ету үшін қосымша шараларды енгізуді талап етеді [6].

2. Қазақстанда АКТ қолданудың қазіргі жағдайы

Қазақстандағы АКТ дамуы жеке тұлғаны сәйкестендіру үдерістеріне айтарлықтай әсер етеді. 2018 жылы іске қосылған «Цифрлық Қазақстан» мемлекеттік бағдарламасы мемлекеттік

басқару, экономика және қауіпсіздік сияқты өмірдің барлық салаларына цифрлық шешімдерді интеграциялауды мақсат етеді. Бағдарламаның негізгі бағыттарының бірі – жеке тұлғаны сәйкестендіру жүйесін жетілдіру үшін АКТ-ны пайдалану болды, бұл құқық қорғау қызметі, мемлекеттік қызметтерді алу және қауіпсіздікті қамтамасыз ету сияқты әртүрлі салалардағы үдерістерді айтарлықтай жеделдетті. Қазақстанда биометриялық сәйкестендіру жүйелерін қолдану цифрлық мемлекетті дамыту стратегиясының маңызды элементіне айналды.

Қазақстанда биометриялық технологияларды қолдану

Қазақстанда биометриялық сәйкестендіру қазіргі уақытта бірнеше негізгі бағыттарда қолданылады:

1. Мемлекеттік қызметтер. Электрондық үкімет (eGov) азаматтарға мемлекеттік қызметтердің кең ауқымын ұсынады. 2020 жылы ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі барлық мемлекеттік қызметтердің 85%-дан астамы eGov жүйесі арқылы көрсетілгенін атап өтті. Жеке тұлғаны растауды жеңілдету үшін Face ID және саусақ іздері сияқты биометриялық технологиялар қолданыла бастады, бұл азаматтардың жеке басын растауға кететін уақытты қысқартуға мүмкіндік берді [6].

2. «Smart City» жобалары. «Ақылды қалалар» тұжырымдамасы (Smart City) қалалардағы қауіпсіздік, экологиялық таза және жайлы өмір сүру деңгейін арттыру үшін АКТ қолдануды қамтиды. Астана мен Алматы алғашқы болып жобаны толық көлемде жүзеге асырған қалалар болды. «Цифрлық Қазақстан» бағдарламасы аясында алдағы жылдары АКТ инфрақұрылымын одан әрі дамыту жоспарланып отыр, бұл биометриялық технологияларды әртүрлі салаларда кеңінен қолдануды да қамтиды [7]. Бет-әлпетті тану функциясы бар бейнебақылау жүйесі қоғамдық орындарда нақты уақыт режимінде мониторинг жүргізуге, сондай-ақ ықтимал қылмыстардың алдын алуға мүмкіндік береді. Мұндай жүйелерді енгізу қоғамдық орындардағы қылмыс деңгейінің 25%-ға төмендеуіне әкелді, бұл туралы Ұлттық ақпараттандыру орталығының деректері дәлелдейді [8].

3. Құқық қорғау органдары. Қазақстанның құқық қорғау құрылымдары күдіктілерді сәйкестендіру, жабық аймақтарға кіруді бақылау және қылмыстық істерді тергеу аясында биометриялық жүйелерді белсенді түрде қолданады. Атап айтқанда, 2021 жылы Астана полициясы биометриялық деректер негізінде адамдарды автоматты түрде сәйкестендіруге мүмкіндік беретін жүйені енгізді, бұл қылмыстарды ашу уақытын едәуір қысқартты [9]. Бұл технологиялар қылмыспен күресу және қоғамдық тәртіпті қамтамасыз етуде маңызды құралға айналууда.

Мәселелер мен сын-қатерлер

АКТ сәтті енгізілгеніне қарамастан, Қазақстанда дербес деректерді қорғау және киберқауіпсіздік мәселелері бойынша шешілмеген бірқатар мәселелер бар. Бұл саладағы негізгі нормативтік-құқықтық акт – «Жеке деректер және оларды қорғау туралы» Заң. Алайда, технологиялардың дамуы және өңделетін биометриялық деректердің көлемінің артуы құқықтық реттеуді жетілдіру қажеттілігін тудырады. 2022 жылы 1200-ден астам дербес деректердің таралуына байланысты киберқылмыс оқиғалары тіркелді, бұл азаматтардың деректерінің қауіпсіздігіне төнетін қауіптердің артқанын көрсетеді [9].

Халықаралық тәжірибеде, атап айтқанда Еуропалық Одақта, деректерді қорғау мәселелері қатаң реттеледі. 2018 жылы қабылданған Деректерді қорғаудың жалпы регламенті (GDPR) биометриялық деректерді өңдеу стандарттарын белгіледі, бұл ақпараттың таралу қаупін және азаматтардың деректерін заңсыз пайдалануды едәуір төмендетуге мүмкіндік берді. Қазақстан Еуропалық Одақтың үлгісі бойынша өз заңнамасын цифрлық дәуірдің жаңа сын-қатерлеріне бейімдеуі тиіс, әсіресе биометриялық ақпаратты қорғау мәселелерінде [8. – 132].

Сонымен қатар, Қазақстан техникалық қиындықтарға тап болып отыр. Күрделі биометриялық жүйелерді енгізу елеулі қаржылық шығындарды, сондай-ақ білікті мамандарды қажет етеді. Инфрақұрылымның және кадрлық әлеуеттің жеткіліксіздігі цифрландыру

процесін баяулатуы мүмкін. АКТ саласындағы мамандарды даярлауға инвестиция салу инновациялық шешімдерді енгізуді жеделдетуге және оларды тәжірибеде тиімді пайдалануға мүмкіндік береді [10].

Даму перспективалары

Қолданыстағы мәселелерге қарамастан, Қазақстанда жеке тұлғаны сәйкестендіру үшін АКТ қолдану перспективалары өте жоғары. Алдағы жылдары көздің торын сканерлеу, дауысты сәйкестендіру және ДНК талдауы сияқты биометриялық технологиялардың одан әрі жетілдірілуі сәйкестендірудің дәлдігін айтарлықтай арттыруға мүмкіндік береді.

Сонымен қатар, Қазақстан халықаралық ұйымдармен ынтымақтастықты және дамыған елдермен тәжірибе алмасуды жалғастырады деп күтілуде, бұл деректерді қорғау және сәйкестендіру жүйелерінің қауіпсіздігін қамтамасыз ету саласындағы озық шешімдерді енгізуге ықпал етеді. Атап айтқанда, Еуропалық Одақпен тәжірибе алмасу және GDPR элементтерін пайдалану Қазақстанда биометриялық сәйкестендіру жүйесін қауіпсіз әрі тиімді ету жолындағы маңызды қадамдар болуы мүмкін.

3. Қазақстанда АКТ арқылы жеке тұлғаны сәйкестендірудің даму перспективалары

АКТ қарқынды дамып келе жатқан жағдайда Қазақстанда жеке тұлғаны сәйкестендіру үдерісін одан әрі жетілдірудің перспективалары айқын бола түсуде. Биометриялық технологиялар, жасанды интеллект, заттар интернеті және басқа да соңғы жетістіктер жеке тұлғаны сәйкестендіру әдістеріне айтарлықтай әсер етуде. Алайда, олардың сәтті енгізілуі мен дамуы елдің заңнамалық базасында және технологиялық инфрақұрылымында тиісті өзгерістерді талап етеді.

Құқықтық реттеудің перспективалары

Құқықтық реттеу жеке тұлғаны сәйкестендіру технологияларын табысты қолданудың негізгі элементі болып табылады. Қазақстандық сарапшылардың пікірінше, қазіргі заңнама цифрлық дәуірдің сын-қатерлеріне бейімделу үшін жаңартуды қажет етеді. Атап айтқанда, «Жеке деректер және оларды қорғау туралы» Заң биометриялық деректерді өңдеудің негізгі қағидаттарын белгілегенімен, жасанды интеллект және заттар интернеті технологияларының жылдам дамуы жағдайында олардың барлық аспектілерін қамтымайды [6. – 55]. Сәйкестендіру жүйелерінің сенімділігін және деректерді қорғауды қамтамасыз ету үшін биометриялық ақпаратты жинау, өңдеу және сақтау бойынша құқықтық бақылау тетіктерін кеңейту, сондай-ақ олардың рұқсатсыз пайдаланылуына жауапкершілікті күшейту қажет.

Халықаралық тәжірибе деректерді қорғау үшін қатаң стандарттарды енгізудің маңыздылығын көрсетеді. Еуропада Деректерді қорғаудың жалпы регламенті (GDPR) биометриялық деректермен жұмыс істеу үшін қатаң құқықтық шеңбер құрды, бұл ақпараттың таралу қаупін және азаматтардың деректерін заңсыз пайдалануды азайтуға мүмкіндік берді. Қазақстан биометриялық ақпараттың қауіпсіздігін қамтамасыз ету және азаматтардың құқықтарын қорғау үшін осындай тәсілдерді бейімдеуі қажет [8. – 132].

Жасанды интеллект пен машиналық оқытудың ықпалы

Қазақстан үшін негізгі перспективалардың бірі – жеке тұлғаны сәйкестендіру жүйелеріне жасанды интеллект (ЖИ) және машиналық оқытуды белсенді енгізу. ЖИ бет-әлпетті, саусақ іздерін және басқа биометриялық параметрлерді танудың дәлдігін және жылдамдығын айтарлықтай арттыра алады. Әсіресе, машиналық оқыту жинақталған деректер негізінде бейімделіп, жетілдіріле алады, бұл сәйкестендіру жүйелерін сенімдірек және тиімдірек етеді [10. – 240].

Қазақстанда сәйкестендіру жүйелерінде ЖИ қолдану «Ақылды қала» бағдарламалары арқылы сәтті жүзеге асырылуы мүмкін. Мысалы, Астана мен Алматы қалаларында бет-әлпетті тану функциясы бар бейнебақылау жүйесі ЖИ элементтерін қолданып, тану дәлдігін жақсартуға және жалған іске қосылуларды азайтуға бағытталған. Болашақта мұндай технологияларды қоғамдық қауіпсіздік саласында ғана емес, медициналық мекемелерде,

банктерде, білім беру ұйымдарында және жеке тұлғаны жылдам және дәл сәйкестендіруді қажет ететін басқа салаларда да қолдануға болады.

Биометриялық технологияларды дамыту

Қазақстанда биометриялық технологияларды қолдану перспективалары өте кең. Қазіргі уақытта көздің торын сканерлеу, дауыс арқылы сәйкестендіру және ДНҚ талдауы сияқты жаңа биометриялық сәйкестендіру әдістері белсенді түрде әзірленуде. Бұл әдістер жеке тұлғаны сәйкестендіру мүмкіндіктерін едәуір кеңейтіп, сәйкестендіру үдерістерінің сенімділігін арттыра алады. Мысалы, халықаралық тәжірибеде қаржы секторында клиенттердің банктік операцияларды жүргізу кезінде дауыс арқылы жеке басын растау үшін сәтті қолданылатын дауыс арқылы сәйкестендіру жүйелері бар [11].

Қазақстанда биометриялық технологияларды дамыту тікелей «Цифрлық Қазақстан» бағдарламасымен байланысты, оның аясында азаматтардың өмір сүру сапасын жақсарту үшін жаңа технологияларды енгізу жоспарлануда. Алдағы жылдары көздің торын тану және ДНҚ талдауы сияқты күрделі биометриялық жүйелерді белсенді енгізу күтілуде, бұл сәйкестендірудің қауіпсіздігі мен дәлдігін арттырады [7. – 48].

Киберқауіпсіздік мәселелері және жеке деректерді қорғау

Биометриялық технологияларды қолданудың артуымен қатар киберқылмыстар қаупі де артып келеді. 2022 жылы ҚР Бас прокуратурасының Құқықтық статистика және арнайы есепке алу комитеті биометриялық деректерді пайдаланатын жүйелерге кибершабуылдар санының айтарлықтай өскенін тіркеді. Осыған байланысты Қазақстанға деректерді қорғау шараларын күшейту, сондай-ақ киберқауіпсіздік инфрақұрылымын дамыту қажет. Халықаралық тәжірибеде мемлекеттер жүйелердің кибершабуылдарға төзімділігін арттыруға бағытталған әзірлемелерге белсенді түрде инвестиция салатын сәтті мысалдар бар [9. – 98].

Киберқауіпсіздік инфрақұрылымын құру және биометриялық ақпаратты қорғау бойынша қатаң заңнамалық шараларды қабылдау цифрлық мемлекеттің толыққанды дамуы жолындағы маңызды қадам болады. Қазақстан ИКТ саласындағы мемлекеттік саясаттың басымдығы ретінде дербес деректерді қорғауды жүзеге асыратын АҚШ және Ұлыбритания сияқты елдердің тәжірибесін ескеруі тиіс [12].

4. Жеке тұлғаны сәйкестендіру үшін АКТ қолданудың халықаралық тәжірибесі

АКТ-ны жеке тұлғаны сәйкестендіру үдерісіне енгізудің халықаралық тәжірибесі дұрыс ұйымдастырылған және құқықтық реттелген жағдайда осы технологиялардың жоғары тиімділігін көрсетеді. Еуропалық Одақ, АҚШ және Қытай елдерінде биометриялық жүйелер мемлекеттік қызметтер мен құқық қорғау органдары жұмысының негізіне айналды.

АҚШ-та бет-әлпетті тану технологиясы «Homeland Security» бағдарламасы аясында белсенді түрде қолданылады, бұл қылмыстардың алдын алуға және шекараларды бақылау жүйесін жақсартуға көмектеседі. 2019 жылы Вашингтон әуежайында бет-әлпетті тану жүйесі бірнеше ай ішінде 100-ден астам құқық бұзушыларды ұстап қалуға мүмкіндік берді [13]. Сонымен қатар, қаржы секторында клиенттерді банктік қызметтерге жедел аутентификациялау үшін биометриялық жүйелер кеңінен қолданылады [11. – 87].

Қытайда әлеуметтік несие жүйесі, оның ішінде бет-әлпетті тану сияқты биометриялық деректерді пайдалану, қоғамдық бақылау жүйесінің маңызды бөлігіне айналды. 2020 жылға қарай ел бойынша азаматтардың қоғамдық қызметін қадағалау үшін 200 миллионнан астам бет-әлпетті тану функциясы бар камералар орнатылды [5. – 140]. Бұл қауіпсіздікті жақсартуға ғана емес, сондай-ақ азаматтардың әлеуметтік несие жүйесі арқылы тәртіптілігін арттыруға мүмкіндік береді.

Еуропалық Одақта, керісінше, басымдық дербес деректерді қорғауға беріледі. 2018 жылы енгізілген Деректерді қорғаудың жалпы регламенті (GDPR) еуропалық елдерде биометриялық ақпаратты өңдеу және сақтау ережелерін қатайтты. Бұл технологиялардың қарқынды дамуы жағдайында азаматтардың құпиялылық құқықтарын қамтамасыз етуде маңызды қадам болды [7. – 132].

5. Қазақстанда АКТ саласындағы құқықтық реттеу

Қазақстанда жеке тұлғаны сәйкестендіру үдерісінде АКТ қолдануды реттеу үшін құқықтық база халықаралық стандарттарға сәйкес қалыптасуда. «Жеке деректер және оларды қорғау туралы» Заң биометриялық деректерді қоса алғанда, дербес деректерді жинау, өңдеу және сақтау мәселелерін реттейтін негізгі нормативтік акт болып табылады.

Қолданыстағы құқықтық база ағымдағы шындықтар мен сын-кәтерлерді тиісті деңгейде көрсету үшін одан әрі жетілдіруді талап етеді. А.А. Бубнов атап өткендей, ақпараттың маңыздылық деңгейі ақпараттың құпиялығы (заңсыз қолжетімдік, көшіру, ұсыну немесе тарату), бүтіндігі (жою немесе түрлендіру) немесе қолжетімдігі (оқшаулау) бұзылу салдарынан ақпаратты иеленушіге (тапсырыс берушіге) және (немесе) операторға келтірілген ықтимал залалдың дәрежесімен анықталады. Ықтимал залал дәрежесін ақпаратты иеленуші, тапсырыс беруші және (немесе) оператор өз бетінше сараптамалық және өзге әдістермен анықтайды [8. – 167].

Егер ақпараттың қауіпсіздік сипаттамаларының (құпиялылық, бүтінді деректерді қорғау саласындағы заңнамалық нормалар биометриялық ақпаратқа рұқсатсыз қол жеткізу және оның таралу қаупіне байланысты нақты тәуекелдерді ескеруі тиіс [6. – 55]. Осыған байланысты Қазақстан Деректерді қорғаудың жалпы регламентін (GDPR) енгізу арқылы жеке деректерді өңдеуді бақылауды айтарлықтай күшейткен Еуропалық Одақ тәжірибесінен сабақ алады.

Қазақстан алдында тұрған мәселелердің бірі – биометриялық деректерді қорғау саласындағы заңнаманың сақталуын бақылау тетіктерін нақтылау қажеттілігі. Деректер операторлары мен сәйкестендіру жүйелеріне қойылатын қатаң талаптарды белгілеу маңызды, бұл азаматтардың құқықтарын қорғауға ықпал етеді.

6. Жеке тұлғаны сәйкестендіру үшін АКТ қолданудың этикалық аспектілері

Этика мәселелері жеке тұлғаны сәйкестендіру үшін биометриялық технологияларды қолдану туралы пікірталастарда маңызды орын алады. Цифрландыру жағдайында азаматтардың қауіпсіздігін қамтамасыз ету және олардың құпиялылық құқықтарын қорғау қажеттілігі арасында дилемма туындайды. Қазіргі ақпараттық-коммуникациялық технология түбегейлі басқа түрі болып табылады барлық алдыңғы технологиялардан өзгеше. Олардың бәріне тән социогендік функциядан басқа, сонымен қатар мәдени және эпистемогендік функциялар бар [9. – 49]. Бет-әлпетті тану және саусақ іздерін сәйкестендіру сияқты биометриялық технологиялар жеке өмірге қол сұғу құқықтарын айтарлықтай бұзуы мүмкін, егер олар тиісті келісімсіз немесе дұрыс емес қолданылса [10. – 150].

Халықаралық тәжірибеде этикалық аспектілер мәліметтерді пайдалануға қойылатын арнайы кодекстер мен нормалар арқылы реттеледі. Мысалы, АҚШ пен ЕО елдерінде этикалық нормалар биометриялық ақпаратты пайдалануда ашықтықты және мәліметтерді минимизациялау қағидасын сақтау — яғни, тек қажетті мәліметтерді жинау талабы белгіленген [11. – 112].

Қазақстанда АКТ қолдану кезінде этика мәселелері барған сайын өзекті бола түсуде. Тұлғаны сәйкестендіру технологияларының тиімділігі мен азаматтардың құқықтарын қорғаудың арасындағы тепе-теңдікті қамтамасыз ету қажет, бұл құқықтық реттеуді жетілдірумен ғана емес, сонымен қатар биометриялық ақпаратты пайдалану саласындағы тәуекелдер мен құқықтар туралы халықты ақпараттандыруды жақсартумен байланысты.

7. Қазақстан мен шетелде АКТ-ны табысты қолданудың жарқын мысалдары

Қазақстанда АКТ-ны қолданудың табысты мысалы ретінде Астана мен Алматы қалаларында жүзеге асырылған «Ақылды қала» жобасын айтуға болады. Бет-әлпетті тану функциясы бар бейнебақылау жүйесі өзінің тиімділігін дәлелдеп, қоғамдық орындардағы қылмыс деңгейін 25%-ға төмендетті [12. – 67]. Бұл жүйе қылмыскерлерді жедел анықтап,

оқиғалардың алдын алу мүмкіндігін қамтамасыз етеді, бұл АКТ-ның қалалық инфрақұрылымға интеграциялануының арқасында мүмкін болды.

Шетелдік тәжірибе де АКТ-ны сәтті қолданудың көптеген мысалдарын ұсынады. Ұлыбританияда CCTV бейнебақылау жүйесі, биометриялық сәйкестендіруді қолдана отырып, Лондон көшелеріндегі қауіпсіздікті қамтамасыз ету үшін белсенді түрде қолданылады. Бұл жүйе терроризм мен ірі ұрлықтарды қоса алғанда, көптеген қылмыстарды ашуға көмектесті [13. – 135]. Финляндияда биометриялық деректер мемлекеттік шекараларда және әуежайларда сәйкестендіру үдерісін жеделдету үшін қолданылады, бұл кезектерді азайтып, азаматтарға көрсетілетін қызметтердің сапасын жақсартуға мүмкіндік береді.

Қорытынды

Жүргізілген зерттеу Қазақстанда жеке тұлғаны сәйкестендіру үшін ақпараттық-коммуникациялық технологияларды қолданудың айтарлықтай әлеуеті бар екенін көрсетті, әсіресе қоғамдық қауіпсіздікті арттыру және мемлекеттік қызметтерді оңтайландыру контекстінде. Бет-әлпетті тану және Face ID сияқты биометриялық технологияларды енгізу ірі қалалардағы қылмыс деңгейін төмендетуде, сондай-ақ әкімшілік үдерістерді жеделдетуде өзінің тиімділігін дәлелдеді.

Соған қарамастан, зерттеу нәтижелері шешуді қажет ететін бірқатар мәселелерді көрсетеді. Негізгі сын-қатерлер жеке деректерді қорғау және киберқауіпсіздікке қатысты, бұл құқықтық реттеуді одан әрі жетілдіруді талап етеді. Қазақстан халықаралық стандарттарды басшылыққа ала отырып, биометриялық ақпаратты қорғауға арналған қатаң заңдарды әзірлеп, Еуропалық Одақта қолданылатын Деректерді қорғаудың жалпы регламенті (GDPR) сияқты үздік тәжірибелерді бейімдеуі маңызды.

Зерттеу сондай-ақ биометриялық технологияларды толыққанды енгізу үшін, әсіресе өңірлерде, Қазақстандағы цифрлық инфрақұрылымды дамытудың қажеттілігін анықтады. Бұл бағыт технологиялық инвестициялармен қатар, осындай жүйелердің қауіпсіздігі мен тиімділігін қамтамасыз ете алатын білікті кадрларды даярлауды талап етеді.

Осылайша, алынған нәтижелер ақпараттық-коммуникациялық технологияларды жеке тұлғаны сәйкестендіру үшін қолдану саласындағы ғылыми білімді кеңейтуге мүмкіндік береді, биометриялық технологиялардың қауіпсіздікті арттыру және мемлекеттік қызметтерді оңтайландыру үшін маңыздылығын көрсетті. Болашақта зерттеу биометриялық деректерді қорғаудың неғұрлым тұрақты модельдерін әзірлеу және көздің торын тану, дауыс арқылы сәйкестендіру сияқты жаңа биометриялық технологияларды зерттеу бағытында тереңдетілуі мүмкін.

ӘДЕБИЕТТЕР ТІЗІМІ:

- 1 Ракитов А.И. Философия компьютерной революции. — М., Изд-во политической литературы. — 1991. — 287 с.
- 2 Влияние GDPR в Казахстане. [Электронный ресурс] — URL: <https://www.dentons.com/en/insights/alerts/2021/may/5/the-impact-of-the-gdpr-in-kazakhstan> (дата обращения: 20.09.2024)
- 3 Тоқаев Қ. Қазақстан Республикасының Президенті Қасым-Жомарт Тоқаевтың Қазақстан халқына Жолдауы. – Нұр-Сұлтан: 2020. [Электрондық ресурс] — URL: https://www.akorda.kz/kz/addresses/addresses_of_president (қаралу уақыты: 23.09.2024)
- 4 Отчет «Исследование МСЭ-D – потенциальные направления развития умных устойчивых городов в регионе СНГ в период 2022-2025». — 61 с.
- 5 Zeng Q. (2019). The Social Credit System in China and the Use of Biometric Data. International Journal of Law and Technology. Vol. 22(3). P. 129-150.
- 6 Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі. 2020 жылғы ҚР-дағы цифрлық технологиялардың даму есебі. Нұр-Сұлтан. ЦДИАӨМ, 2020. — 156 б.
- 7 Еуропалық парламент пен кеңестің 2016 жылғы 27 сәуірдегі №2016/679 ережесі (Жалпы мәліметтерді қорғау ережесі). – Еуропалық Одақтың ресми журналы. — Т. 59(4). — Б. 1-88.
- 8 Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности: учебное издание. – М.: «Академия» баспа. — No 2. — 2016. – 256 с.

- 9 Удовик В.Е. Роль информационно-коммуникационных технологий в современном обществе. М.: МГТУ «МАМИ». — 2010. — 6 с.
- 10 Smith J. (2019). New Directions in Biometric Identification – Oxford: Oxford University Press. 340 p.
- 11 Smith J., Brown T. (2020). The Global Impact of Biometric Identification. New-York: Palgrave Macmillan. 320 p.
- 12 ҚР Бас прокуратурасының Құқықтық статистика және арнайы есепке алу комитеті. 2022 жылғы ҚР-дағы киберқылмыстар статистикасы. – Нұр-Сұлтан: ҚР Бас прокуратурасы. — 2022. – 112 б.
- 13 Johnson, P. Adams. (2021). Cybersecurity and Data Protection in the United Kingdom. London: Routledge. 276 p.

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация

Статья посвящена исследованию применения информационно-коммуникационных технологий (ИКТ) для идентификации личности в Казахстане, а также анализу правового регулирования и защиты биометрических данных. В статье рассмотрены современные технологии идентификации, включая системы распознавания лиц и отпечатков пальцев, которые активно используются в рамках программы «Цифровой Казахстан». Особое внимание уделено анализу правовой базы Казахстана в области защиты персональных данных и кибербезопасности, а также необходимости совершенствования существующего законодательства.

Методологическая основа исследования включает анализ нормативно-правовых актов, статистических данных о снижении уровня преступности в крупных городах, а также сравнительный анализ международного опыта использования ИКТ. В статье представлены результаты использования биометрических систем в городах Астана и Алматы, где отмечено снижение преступности на 20-25% благодаря внедрению технологий распознавания лиц. Основные проблемы, выявленные в ходе исследования, включают недостаточную правовую защиту биометрической информации и уязвимость к кибератакам.

Теоретическая значимость исследования заключается в развитии научных представлений о роли ИКТ в процессе идентификации личности, а также в анализе правовых и этических аспектов использования биометрических данных. Практическая значимость работы заключается в предоставлении рекомендаций по совершенствованию законодательства Казахстана, направленных на усиление защиты персональных данных и развитие цифровой инфраструктуры. В статье также выделены направления для дальнейших исследований, включая изучение новых методов биометрической идентификации и разработку механизмов кибербезопасности.

Ключевые слова: идентификация личности, информационно-коммуникационные технологии, биометрические данные, защита персональных данных, распознавание лиц, кибербезопасность, правовое регулирование.

THE CURRENT STATE AND PROSPECTS FOR DETERMINING THE PERSONALITY OF A PERSON THROUGH INFORMATION AND COMMUNICATION TECHNOLOGIES

Abstract

This article explores the use of information and communication technologies (ICT) for personal identification in Kazakhstan, as well as the legal regulation and protection of biometric data. The article examines modern identification technologies, including facial recognition and fingerprint systems, which are actively used within the framework of the "Digital Kazakhstan" program. Special attention is paid to the analysis of Kazakhstan's legal framework in the field of personal data protection and cybersecurity, as well as the need to improve existing legislation.

The methodological basis of the study includes an analysis of legal acts, statistical data on crime reduction in major cities, and a comparative analysis of international practices in the use of ICT. The article presents the results of the use of biometric systems in Nur-Sultan and Almaty, where a 20-25% reduction in crime rates was observed due to the implementation of facial recognition technologies. The main issues identified during the study include insufficient legal protection of biometric information and its vulnerability to cyberattacks.

The theoretical significance of the study lies in the development of scientific understanding of the role of ICT in the process of personal identification, as well as the analysis of legal and ethical aspects of the use of biometric data. The practical significance of the work lies in providing recommendations for improving Kazakhstan's legislation aimed at strengthening personal data protection and developing digital infrastructure. The article also highlights directions for further research, including the study of new biometric identification methods and the development of cybersecurity mechanisms.

Key words: personal identification, information and communication technologies, biometric data, personal data protection, facial recognition, cybersecurity, legal regulation.

REFERENCES

- 1 Rakitov A.I. *Filosofiya komp'yuternoj revolyucii [Philosophy of the computer revolution]*. M. Izd-vo politicheskoy literatury. 1991. 287 p. [in Russian].
- 2 Vliyanie GDPR v Kazahstane [*Impact of GDPR in Kazakhstan*]. Available at – URL: <https://www.dentons.com/en/insights/alerts/2021/may/5/the-impact-of-the-gdpr-in-kazakhstan> [in Russian]. (accessed: 20.09.2024).
- 3 Toqaeв Q. Qazaqstan Respublikasynyń Prezidentі Qasym-Jomart Toqaevtyń Qazaqstan halqyna Joldaуy [*Address of the president of the Republic of Kazakhstan Kassym-Jomart Tokayev to the people of Kazakhstan*]. Nūr-Sūltan: 2020. Available at – URL: https://www.akorda.kz/kz/addresses/addresses_of_president [in Kazakh] (accessed: 23.09.2024)
- 4 Otchet «Issledovanie MSE-D – potencial'nye napravleniya razvitiya umnyh ustojchivyh gorodov v regione SNG v period 2022-2025». [*ITU-D study - potential directions for the development of smart sustainable cities in the CIS region in the period 2022-2025*]. 61 p. [in Russian].
- 5 Zeng Q. (2019). The Social Credit System in China and the Use of Biometric Data. *International Journal of Law and Technology*. Vol. 22(3). P. 129-150. [in English].
- 6 Qazaqstan Respublikasynyń Sifirlyq damu, innovasiolar jәne aeroğarys önerkәsibі ministrlyğy. 2020 jylğy QR-dağy sifirlyq tehnologialardyń damu esebі [*Report on the development of digital technologies in the Republic of Kazakhstan in 2020*]. Nūr-Sūltan. SDIAÖM. 2020. 156 p.
- 7 Europalyq parlament pen keñestіñ 2016 jylğy 27 säuirdegi №2016/679 erejesі (Jalpy мәліметтерді қорғау erejesі) [*Regulation No. 2016/679 of the European Parliament and Council of 27 April 2016 (General Data Protection Regulation)*]. Europalyq Odaқтыń resmi jurnaly. Vol. 59, No. 4. P. 1-88. [in Kazakh]
- 8 Bubnov A.A., Przhegorlinskij V.N., Savinkin O.A. *Osnovy informacionnoj bezopasnosti: uchebnoe izdanie [Fundamentals of information security: a textbook]*. M.: «Akademiya» baspa. No 2. 2016. 256 p. [in Russian].
- 9 Udovik V.E. Rol' informacionno-kommunikacionnyh tekhnologij v sovremennom obshchestve [*The role of information and communication technologies in modern society*]. M.: MGTU «MAMI». 2010. 6 p. [in Russian].
- 10 Smith J. (2019). *New Directions in Biometric Identification* – Oxford: Oxford University Press. 340 p. [in English].
- 11 Smith J., Brown T. (2020). *The Global Impact of Biometric Identification*. New-York: Palgrave Macmillan. 320 p. [in English].
- 12 QR Bas prokuraturasynyń Qūqyqtyq statistika jәne arнай esepke alu komitetі [*Committee on Legal Statistics and special accounts of the prosecutor general's Office of the Republic of Kazakhstan*]. 2022 jylğy QR-dağy kiberqylmystar statistikasy. – Nūr-Sūltan: QR Bas prokuraturasy. 2022. 112 p.[in Kazakh]
- 13 Johnson, P. Adams. (2021). *Cybersecurity and Data Protection in the United Kingdom*. London: Routledge. 276 p. [in English].

Information about authors:

Aitolkyn Doszhanova – **corresponding author**, 2nd-year doctoral student, Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan, Kosshy, Republic of Kazakhstan

E-mail: aitok82@mail.ru

ORCID: <https://orcid.org/0009-0007-3257-6601>

Dina Bugybay – candidate of legal sciences, associate professor of the Department of “Law”, Acting Professor, Sh. Yessenov University of Caspian Technologies and Engineering, Aktau, Republic of Kazakhstan

E-mail: Bugibaid@mail.ru

ORCID: <https://orcid.org/0000-0002-2777-7739>

Информация об авторах:

Айтолкын Досжанова – **основной автор**, докторант 2-го курса, Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан

E-mail: aitok82@mail.ru

ORCID: <https://orcid.org/0009-0007-3257-6601>

Дина Бұғыбай – кандидат юридических наук, доцент кафедры «Юриспруденция», и.о. профессора, Каспийский университет технологий и инжиниринга имени Ш. Есенова, г. Актау, Республика Казахстан

E-mail: Bugibaid@mail.ru

ORCID: <https://orcid.org/0000-0002-2777-7739>

Авторлар туралы ақпарат:

Айтолқын Досжанова - **негізгі автор**, 2-курс докторанты, Қазақстан Республикасы Бас прокуратурасы жанындағы құқық қорғау академиясы, Косшы қ., Қазақстан Республикасы

E-mail: aitok82@mail.ru

ORCID: <https://orcid.org/0009-0007-3257-6601>

Дина Бұғыбай – заң ғылымдарының кандидаты, «Құқықтану» кафедрасының доценті, профессордың м.а., Ш.Есенов атындағы Каспий технологиялар және инжиниринг университеті, Ақтау қ., Қазақстан Республикасы

E-mail: Bugibaid@mail.ru

ORCID: <https://orcid.org/0000-0002-2777-7739>