УДК 51-76; 004.20 **https://doi.org/10.58805/kazutb.v.2.15-2**

Г.З. Зиятбекова[1,2], М.С. Әлиасқар[2], Ә.Т. Мазақова[1,2], М.Ә. Шайхы[2]
[1]Қазақстан Республикасының Білім және Ғылым Министрлігі Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан,
[2]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,
e-mail: ziyatbekova@mail.ru

БИОМЕТРИЯЛЫҚ ТЕХНОЛОГИЯ ЖҰМЫСЫНЫҢ СИПАТТАМАСЫ

Аңдатпа. Мақала адамның биометриялық сәйкестендіру жүйесін құруға арналған. Биометриялық аутентификация және жеке сәйкестендіру әдістеріне шолу жасалды. Саусақ іздері мен адамның беті биометриялық ақпарат көзі ретінде қарастырылады. Биометриялық технологияның тиімділігін анықтайтын негізгі параметрлер сипатталған, сынақ базасы келтірілген, соған сәйкес бұл параметрлер анықталады. Параметр мәндерін таңдау бойынша ұсыныстар мен критерийлер тұжырымдалған.

Түйін сөздер: биометрия, аутентификация, сәйкестендіру жүйесі, саусақ ізі, критерий, FAR мәні.

Г.З. Зиятбекова[1,2], М.С. Әлиасқар[2], Ә.Т. Мазақова[1,2], М.А. Шайхы[2]
[1]Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан, [2]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан, e-mail: ziyatbekova@mail.ru

ХАРАКТЕРИСТИКА РАБОТЫ БИОМЕТРИЧЕСКОЙ ТЕХНОЛОГИИ

Аннотация. Статья посвящена созданию системы биометрической идентификации человека. Проведен обзор по методам биометрической аутентификации и идентификации личности. В качестве источников биометрической информации рассмотрены отпечатки пальцев и лицо человека. Описываются основные параметры определяющие, эффективность работы биометрических технологий, приведена тестовая база, по которой определяются эти параметры. Сформулированы рекомендации и критерии выбора значений параметров.

Ключевые слова: биометрия, аутентификация, система идентификации, отпечаток пальца, критерий, значение FAR.

G.Z. Ziyatbekova[1,2], M.S. Aliaskar[2], A.T. Mazakova[1,2], M.A. Shaikhy[2]
[1]RSE Institute of Information and Computational Technologies MES RK CS,
Almaty, Kazakhstan, [2]Al-Farabi Kazakh National University, Almaty,
Kazakhstan, e-mail: ziyatbekova@mail.ru

CHARACTERISTICS OF THE BIOMETRIC TECHNOLOGY

Abstract. The article is devoted to the creation of a system of biometric identification of a person. A review was made on the methods of biometric authentication and personal identification. Fingerprints and a person's face are considered as sources of biometric information. The main parameters that determine the effectiveness of the biometric technology are described, the test base is given, according to which these parameters are determined. Recommendations and criteria for choosing parameter values are formulated.

Keywords: biometrics, authentication, identification system, fingerprint, criterion, FAR value.

Кіріспе. Дербес деректер – тегі, аты, әкесінің аты, туған жылы, айы, күні мен туған жерін қоса алғанда, нақты немесе осындай ақпарат негізінде айқындалатын жеке тұлғаға (дербес деректер субъектісіне) қатысты кез келген ақпарат. жеке басы, мекен-жайы, отбасы, әлеуметтік, мүліктік жағдайы, білімі, кәсібі, кірісі және тағы басқа ақпараттар жатады.

Биометриялық жеке деректер – бұл адамның физиологиялық және биологиялық ерекшеліктерін сипаттайтын ақпарат, оның негізінде тұлғаның жеке басын анықтауға болады. Биометриялық ақпарат – бұл жеке мәліметтерге қатысты әлеуметтік құндылыққа ие болатын биологиялық ақпарат. Биометриялық дербес деректер биометриялық құжатқа енгізіледі, ол адамның жеке басын дәл анықтауға мүмкіндік береді [1].

Биометриялық дербес деректерге: саусақ іздері деректері, көздің нұрлы қабығы, ДНҚ тестілері, бойы, салмағы, адамның бейнесі (фотосурет) жатады. Алайда, кәдімгі фотосурет тек жеке басын анықтау үшін қолданылады, яғни аутентификация және сәйкестендіру үшін пайдаланылмайды. Кәдімгі фотосурет биометриялық жеке деректер емес, тек азаматтың бейнесі болып табылады. Фотографиялық кескінді биометриялық жеке деректермен тікелей байланыстыратын нормативтік құқықтық актілердің ережелері бар. Сонымен қатар, төлқұжаттағы биометриялық жеке деректерді, соның ішінде фотографиялық кескінді өңдеу кезінде оператордың мақсаты ескерілуі керек.

Сондай-ақ, қызметкерлердің, мемлекеттік органдардың, кәсіпорындардың (ұйымдардың) келушілерінің электрондық өткізу құжаттарындағы фотографиялық бейнелері биометриялық жеке мәліметтер болып табылады, өйткені олар адамның физиологиялық және биологиялық ерекшеліктерін сипаттайды, бұл берілген рұқсаттың осы адамға тиесілі немесе тиесілі емес екенін анықтауға мүмкіндік береді. Фотографиялық суреттерді фотосуреттің иесінің тұлғасымен салыстыру арқылы жеке басын анықтау үшін пайдалануға болады. Бұл биометриялық деректерді оператор рұқсаттаманы оның нақты иесі ұсынғанына күмән

болған жағдайда дербес деректер субъектісінің жеке басын анықтау үшін пайдаланады. Осылайша, идентификация жасалатын аумаққа бір немесе бірнеше рет кіруді қамтамасыз ету және азаматтың жеке басын сәйкестендіру үшін пайдаланылатын биометриялық деректер биометриялық жеке деректер деп аталады.

Әдістер мен материалдар. Эксперименттік зерттеулердің әдістемесі қарастырылып, сәйкестендіру нәтижелерін өңдеу процесі сипатталады.

Тұлғаның төлқұжаты белгілі бір адамның қандай да бір әрекеттерді жүзеге асырғанын растау үшін (мысалы, банктік, медициналық және т.б. қызметтерді көрсету туралы келісім-шарт жасасу) сәйкестендіру (жеке басын анықтау) процедураларынсыз болған жағдайда, бұл әрекеттерді биометриялық жеке деректерді өңдеу деп санауға болмайды.

Биометриялық жеке мәліметтер – қызметкердің жеке ісіндегі адамның қолы. Олардың барлығы биометриялық жеке деректер болып саналмайды. Себебі бұл деректер олардың жеке басы анықталған және жеке деректері оператордың иелігінде болған нақты жеке тұлғаға тиесілі екенін растау үшін қолданылады. Адамның физиологиялық және биологиялық ерекшеліктерін сипаттайтын және пациенттің ауру тарихындағы (медициналық картадағы) рентген немесе флюорографиялық суреттер (маңызды емес, қағаз немесе электронды) биометриялық жеке деректер болып табылмайды, өйткені оларды оператор (медициналық мекеме) пациентті сәйкестендіру үшін пайдаланбайды. Бірақ олар жедел-іздестіру қызметі субъектілерінің, тергеу және анықтау органдарының сұрау салуы бойынша олар жүргізетін іс-шаралар шеңберінде берілген жағдайда, көрсетілген ақпарат биометриялық дербес деректерге айналады, адамның жеке басын анықтау мақсатында немесе оны тергеу және ведомстволық операциялар жасауда пайдаланады.

Талқылау. Биометриялық сәйкестендіру жүйесінде саусақ іздері туралы ақпаратты өңдеу аралық бетіндегі папиллярлық өрнектердің бейнесін сандық түрге айналдыру және алынған деректерді биометриялық ақпарат үлгісі түрінде дерекқорға орналастыру арқылы жүзеге асырылады. Осылайша, биометриялық деректерді белгілі бір адамның жеке басын сәйкестендіруге бағытталған оператор жүзеге асыратын қызмет аясында ғана биометриялық жеке деректер ретінде жіктеуге болады.

Қазіргі уақытта қылмыс пен терроризмге қарсы күрестің күшеюіне, қауіпсіздік индустриясының өсуін ынталандыруға байланысты биометриялық технологияларды қолдана отырып жүзеге асырылатын жеке тұлғаны сәйкестендіру ең перспективалы және тез дамып келе жатқан бағыттардың бірі болып табылады. Биометриялық әдістер мен жеке сәйкестендіру құралдарының арасында биометриялық (дактилоскопиялық) жүйелер жетекші орын алады. Бұл зерттеуде олардың сапасын сандық бағалау қарастырылады.

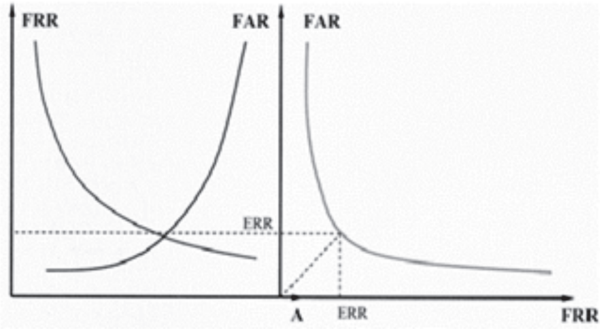
Саусақ ізін салыстыру алгоритмінің сапасын бағалау үшін жасалған жүйелердің сенімділігін анықтайтын сандық көрсеткіштерді алу үшін оңай қолдануға болатын сипаттамалар бар. Бұл сипаттамалар бірінші және екінші типтегі қателіктердің болуымен бірге жүреді.

Бірінші типтегі қате “дос” және “дос емес” салыстырған кезде пайда болады, егер “дос емес” бөтен деп танылса, ол FRR (жалған ауытқу коэффициенті) ретінде белгіленіп, бірінші типтегі қателіктің ықтималдығы болады, яғни өзіміздегі адамды жоқ деп тану ықтималдығы. Бұл жағдайда бірінші типтегі қатенің қарама-қарсы сипат-

тамасы бар: GAR (шынайы қабылдау коэффициенті) = FRR, “өзіңдікін” өткізіп жіберу мүмкіндігі.

Екінші типтегі қате “бөтен” мен “бөтен емес”-ті салыстырған кезде, “бөтен” идентификациядан өтіп, “дос” деп танылған кезде пайда болады. Ол FAR (жалған қабылдау коэффициенті) ретінде белгіленіп, екінші типтегі қателіктің ықтималдығы, яғни біреудің жіберіп алу мүмкіндігі болып саналады. Алгоритмді жан-жақты бағалау үшін EER (Equal Error Rate) параметрі бар, ол – FAR және FRR тең болатын биометриялық қол жетімділік жүйесінің қателік деңгейі [2].

FAR, FRR, FAR және EER ұпайларын тестілеу үшін саусақ ізі туралы арнайы мәліметтер базасын дайындау қажет. Бұл сипаттамалардың дәлдігі оның мөлшеріне байланысты болады. Мұндай мәліметтер базасы әр түрлі саусақтардың n (саусақ саны) және M (үлгілер саны) әр саусақтың саусақ ізі нұсқаларынан тұрады, яғни дерекқордағы саусақ іздерінің жалпы саны (n×m) болады.



Сурет 1– FAR, FRR, FAR және EER нүктелерін картасы

FRR – бірінші типтегі қателіктің ықтималдығы;
FAR – екінші типтегі қателік ықтималдығы;
A – анықтаудың шекті мәні;
ERR – ықтималдық теңдігі нүктесі.

Саусақ іздерінің сынақ базасын құру кезінде синтезделген саусақ іздерін пайдалану алгоритм сапасының нақты көрінісін алуға мүмкіндік бермейтінін ескеру қажет. Осылайша, әр түрлі типтегі нақты басып шығарудың үлкен негіздерін жинау керек. Бұл процедураны жеңілдету үшін тесттік мәліметтер базасының көлемін едәуір азайтуға мүмкіндік беретін бірқатар алгоритмдерді қолдануға болады [2].

Мысалы, бірінші типтегі қателіктер статистикасын алу үшін «дос» түрін «бөтен» түрімен салыстыруды қамтамасыз ету үшін бір жолдың іздері арасында жұптасып салыстыру қажет. Егер жолдағы бірінші саусақ ізі жолдағы барлық саусақ іздерімен салыстырылса, онда (m-1) салыстыру алынады; жолдағы екінші саусақ ізін одан кейінгі барлық іздермен салыстырыңыз, өйткені ол бірінші басып шығарумен салыстырылды, біз (m-2) салыстыруды аламыз және т.с.с. соңғы саусақ ізі тек соңғы саусақ ізімен салыстырылады да бір салыстыру алынады. Осылайша, сериядағы салыстырулар саны мынаған тең болады:

$$V_1 = (m-1) + (m-2) + \mathrm{K} + 1 = \frac{m\,(m-1)}{2}$$

Егер жолдардың саны n болса, онда m саусақ іздері бар N саусақ базасында “дос” пен “дос емес” салыстырудың мүмкін саны тең болады:

$$\mathrm{VFRR} = \frac{nm\,(m-1)}{2}$$

Екінші типтегі қателіктер статистикасын алу үшін “бөтен” түрін “бөтен емес” түрімен салыстыруды қамтамасыз етіп, әр түрлі сериялардың саусақ іздері арасында жұптасып салыстыру қажет.

Бірінші қатардың бірінші ізі барлық қалған қатарлардың барлық іздерімен са-

лыстырылады және салыстырулар (n-1)×m алынады; бірінші қатардың екінші ізі де салыстырылады, ал (n-1)×m салыстырулар көп болады. Бірінші қатардағы басып шығаруларды басқа жолдардың барлық басып шығаруларымен салыстырғаннан кейін біз M2×(n-1) салыстыруды аламыз.

Екінші қатардағы іздер одан кейінгі барлық (n-2) жолдардың ізімен салыстырылады, өйткені олар бірінші қатардағы іздермен салыстырылды және біз m2×(n-2) салыстыруды көбірек аламыз. Бұл процедура тек бір, соңғы қатармен салыстырылатын соңғы қатарға дейін орындалады және біз M2 салыстыруды көбірек аламыз. Бұл дегеніміз, "бөтен" мен "бөтен емес" арасындағы салыстырулардың саны N саусақ іздері бар мәліметтер базасында болады:

$$VFRR = m2\,[(n-1) + (n-2) + K + 1] = = \frac{m^2\, n\,(n-1)}{2}$$

Осылайша, мысалы, 350 саусақ базасында әр саусақ ізінің 6 нұсқасы бар (Сурет 2). Бұл әдісті қолдану тест базасында саусақ іздерінің салыстырмалы түрде аз санымен сипаттамаларды құру үшін қажетті салыстыру нұсқаларының жеткілікті үлкен санын алуға мүмкіндік береді.

Сурет 2 – Сканерлеу кезінде саусақ ізінің әртүрлі позицияларының мысалы

Қажетті FAR және FRR мәндерін таңдау критерийлерін тұжырымдауды бастамас бұрын, әр параметрдің рөлін тағы бір рет талдап көрейік.

Бір жағынан, FRR-дің жоғары мәні ("өздерін" қате ұстау ықтималдығы) жүйенің беделін түсіруге және оның жұмыс істеу тиімділігінің төмендеуіне әкелуі мүмкін, өйткені жиі жалған дабылдармен қауіпсіздік қызметкерлері кідірістерге немесе қол жеткізуден бас тартуға назар аудармайды. Екінші жағынан, әділ құнның жоғары болуы ("бөтен адамды" қате жіберіп алу мүмкіндігі) рұқсатсыз кіру мүмкіндігін арттырады. FAR, FRR-дің белгіленген анықтау шектеріне тәуелділігін ескере отырып, объектінің қауіпсіздік жүйесінің әкімшісі үшін шекті мәндерді таңдау міндеті өте өзекті екенін атап өткен жөн. Біз қажетті мәндерді таңдау әдістерін анықтау және оларды әрі қарай оңтайландыру жолдарын ұсынуға тырысамыз [3].

Ол үшін жүйенің жұмысы мен дамуы кезінде қандай параметрлерді орнату керектігін және қайсысын жақсарту керектігін анықтаймыз. Параметрдің мәнін таңдау критерийлері кез-келген автоматтандырылған қауіпсіздік жүйесіне тең беріктік, аудандастыру, бейімделу, сәйкестік, сенімділік және басқару принциптері негізінде құрылғанын анықтайтын нормативтік құжаттардың талаптарына негізделуі керек.

Тең күш принципі физикалық күш мәндері мен қорғалатын аумақтың бүкіл шекарасында анықтаудың ықтималды сипаттамалары арасындағы тепе-теңдікті қамтиды. Өздеріңіз білетіндей, шекара – бұл объектінің периметрі мен бақылау-өткізу пунктінде орналасқан күзет дабылы, теледидарлық бақылау, кіруді бақылау және инженерлік қорғау. Осылайша, осы талапты басшылыққа ала отырып, бақылау-өткізу пунктінде құқық бұзушыны анықтау ықтимал-

дығы, кем дегенде, периметрдегі анықтау ықтималдығымен салыстырылуы керек деп болжауға болады (физикалық қауіпсіздік шекараларын сипаттайтын параметрлердің шамамен тең болу шарттары сақталған кезде). Периметрде табу ықтималдығы P, содан кейін FAR мәні формула бойынша анықталады делік: FAR = 1 – P.

Мыналарды қосыңыз:

– уәкілетті емес адамды автоматты ұстауды қамтамасыз ететін шлюздік (блоктау) технологияларды пайдалану;

– ұстау жағдайларын бейне растау және бейнеқұжаттау;

– биометриялық параметрлерді ұсынудың бір ғана әрекеті рұқсат етіледі;

– биометриялық бақылау рәсімдерінің басқа, оның ішінде берілген сипаттамалар (кодтар, парольдер және т.б.) бойынша есептік деректерді тексерумен үйлесуі.

Егер сіз far құнын бағалаудың ұсынылған әдісін басшылыққа алсаңыз, онда аймақтық құрылыс және жеткіліктілік принципі айқын болады да, ол таңдалған FAR мәніне де әсер етеді. Сақтау қажеттілігі биометриялық жүйе параметрлерінің бейімделу және басқару принциптері. Бұл жағдайда бейімделу қолданылатын жүйеде анықтау шектерін өзгерту мүмкіндігінің міндетті түрде болуын болжайды [4].

Басқару принципі, ең алдымен, FAR және FRR есептеу құралдарының болуымен қамтамасыз етілуі керек. Сонымен қатар, far есептеу үшін анықтау шегі өзгерген кезде мәліметтер базасында сақталған "стандарттар" әдісімен "бөтен" әдісті "бөтен" әдіспен салыстыру үшін математикалық аппаратты қолданған жөн.

FRR-ді бағалау үшін "биометриялық бақылаудан өткен жоқ" критерийі бойынша қол жеткізуден бас тарту санының биометриялық параметрлерді көрсету әрекеттерінің жалпы санына қатынасын пайдаланған жөн.

Өкінішке орай, жүйені алғаш іске қосқан кезде, FRR-ді көрсетілген әдіспен немесе "дос"-ты "дос емес"-пен салыстыру арқылы анықтауға арналған деректер жүйеде нақты себептермен қол жетімді емес.

Осылайша, far мәнін міндетті жүйелік параметр ретінде және осылайша анықтау шегі ретінде орната отырып, біз жаппай өту жүйесін қосамыз.

Өңделетін үлкен массивтерде кездесетін биометриялық жүйелердің тиімділігін бағалау ерекшеліктері қарастырылады. Бұл көрсетілген:

1) саусақ іздерінің сынақ базасын құру кезінде синтезделген саусақ іздерін пайдалану алгоритмі сапасының нақты көрінісін алуға мүмкіндік бермейтіндігін ескеру қажет;

2) тесттік мәліметтер базасының көлемін едәуір азайтуға мүмкіндік беретін бірқатар алгоритмдерді қолдануға болады;

3) биометриялық жүйе параметрлерінің бейімделу және басқару принциптерін сақтау қажет;

4) аймақтық құрылыс және барабарлық қағидаты таңдалған әділ құнға да әсер етеді.

Ақпаратты қорғау және ақпараттық қауіпсіздік мәселесі қазіргі қоғам дамуының маңызды аспектілерінің бірі болып табылады. Қазіргі уақытта әртүрлі мақсаттағы ақпараттық жүйелерді (әскери, техникалық, экономикалық, медициналық, әлеуметтік және т.б.) әзірлеу және пайдалану кезінде бұл мәселені шешу олардың қауіпсіздігін қамтамасыз ету және рұқсатсыз кіруден бағдарламалық және аппараттық құралдарды құру бойынша барлық талаптарды әзірлеуге байланысты [5].

Сәйкестендіру үшін бетті автоматты түрде тану әртүрлі салаларда көптеген қосымшаларға ие. Қоғамдық қауіпсіздік мәселе-

лері, қашықтан аутентификация қажеттілігі және адам-машина интерфейстерінің дамуы осы технологияға деген қызығушылықты арттырады. Маңыздысы, көптеген жағдайларда бетті танудың қолайлы сапасына қол жеткізу үшін қымбат арнайы жабдық қажет емес: үлгілердің көздері кәсіби емес камера түсірген фотосуреттер немесе бейнелер болуы мүмкін. Бет бейнесі – көптеген әлеуметтік және файл алмасу желілерінің арқасында адамның ең көп таралған және қол жетімді биометриялық параметрлерінің бірі. Бұл факт биометриялық мәліметтерге негізделген ғаламдық Интернет желісінде ақпарат табуға байланысты міндеттердің жаңа түрін тудырды.

Бетті тану әдістерін әзірлеу бірнеше ондаған жылдар бойы жүргізіліп келеді, бірақ бұл мәселе әлі аяқталған жоқ. Жарықтандыруға, бастың камераға қатысты орналасуына, қартаюға, бет әлпетіне және басқа факторларға байланысты бет-әлпеттің өзгеру жағдайларына байланысты, бетті автоматты түрде тану оңай емес. Адамдарды суретке түсіру процесіне қатаң шектеулер қоя отырып, жүйелерді жобалау кезінде олар осы факторлардың теріс әсерінен аулақ болуға тырысады. Алайда, ең үлкен практикалық қызығушылық – бақыланбайтын жағдайда алынған суреттердегі бет-әлпетті тану мәселесі. Машиналық оқыту әдістерінің дамуы және оқыту жүйелері үшін үлкен фото дерекқорлардың пайда болуы соңғы жылдары осы салада айтарлықтай жетістіктерге жетті.

Суреттердегі адамдарды анықтау және локализациялау алгоритмдерін құру бақыланбайтын жағдайларда алынған бейнелердегі адамдарды автоматты түрде сәйкестендіру мәселесін шешуді қамтиды. Негізгі компоненттерді талдау және ықтималды сызықтық дискриминантты талдау соңғы бірнеше жыл ішінде бет-әлпетті модельдеудің басым тәсілдері болды.

Адамды биометриялық сәйкестендіру әдістері жұмыс орындарына, мобильді құрылғыларға, жергілікті және жаһандық ақпараттық ресурстарға қол жеткізуді басқару жүйелерінде кеңінен қолданылады. Жүйелерді енгізу үшін арнайы жабдық қажет емес және биометриялық сипаттаманы жоғалту, ұмыту немесе беру мүмкін емес болғандықтан, ең перспективалы жүйелер болып табылады, олардың жұмыс принципі адамның бет-әлпетін тануға негізделген.

Қазақстан Республикасы Президентінің 2006 жылғы 10 қазандағы №199 Жарлығында "Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы" атап көрсетіледі: Қазақстандағы ақпараттық қауіпсіздіктің ағымдағы жай-күйін талдау оның деңгейі қазіргі уақытта адамның, қоғамның және мемлекеттің "ақпараттық қауіпсіздік жүйелері, оның ішінде мемлекеттік ақпараттық ресурстардағы" қажеттіліктеріне сәйкес келмейтінін көрсетеді.

2017 жылғы 31 қаңтарда Қазақстан Республикасының Президенті Нұрсұлтан Әбішұлы Назарбаев Қазақстан халқына "Қазақстанның Үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік" жолдауын арнады. Бұл үндеуде "Цифрлық Қазақстан" бағдарламасын әзірлеу және қабылдау қажеттілігі атап өтілді. Осыған байланысты атынан Н.Ә. Назарбаев, ақпараттандыру және коммуникация саласында қоғам мен мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ету, сондай-ақ ақпараттық-коммуникациялық технологияларды пайдалану кезінде азаматтардың жеке өмірін қорғау мақсатында "Қазақстанның киберқауіпсіздік" тұжырымдамасы әзірленді. Онда Қазақстан университеттерінде ақпараттық қауіпсіздік мәселелері бойынша кадрлар даярлау және ақпараттық қауіпсіздіктің отандық құралдарын әзірлеу ерекше назар аударуды талап ететіні атап өтілді [6].

Осылайша, ақпаратты қорғаудың өзекті міндеттерінің бірі – жеке басын сәйкестендіру және сәйкестендіру мәселесі. Пайдаланушыны аутентификациялау мәселесін шешудің үш тәсілі бар. Қазіргі уақытта жеке басын сәйкестендірудің үш дәстүрлі әдісі қолданылады:

– меншік бойынша: кілт, төлқұжат, смарт-карта сияқты физикалық заттар;

– білім бойынша: құпияда сақталатын және құпия сөз сияқты белгілі бір адам ғана білетін ақпарат;

- биометриялық параметрлер бойынша: адамның физиологиялық немесе мінез-құлық сипаттамалары. Бұл адам денесінің мүшелері мен бөліктерінің құрылымының жеке ерекшеліктері немесе адамдарды бір-бірінен ажыратуға болатын белгілі бір адамға тән әрекеттер [8].

Аппараттық аутентификация. Пайдаланушылардың қауіпсіз аутентификациясы үшін бірнеше факторларды ескеру қажет. Әдетте көп факторлы аутентификация үшін қолданылатын смарт-карталар немесе аппараттық токендер инициализациялау, тарату және техникалық қызмет көрсету шығындарын талап етеді. “Аппараттық” аутентификацияның кемшіліктері: затты оның иесінен ұрлауға болады, арнайы жабдықтың талабы, арнайы бағдарламалық жасақтаманың талабы, заттың көшірмесін немесе эмуляторын жасау мүмкіндігі.

Пароль аутентификациясы. Бүгінгі таңда парольмен қорғау ақпараттық жүйелерге кіру кезінде адамды аутентификациялаудың негізгі әдісі болып қала береді. Пароль мен аутентификация ең көп таралған: біріншіден, бұл біз қарастыратын аутентификация әдістерінің ішіндегі ең қарапайымы, екіншіден, ол басқалардан әлдеқайда ертерек пайда болды, сондықтан қазір көптеген компьютерлік бағдарламаларда жүзеге асырылуда. Кәдімгі парольдерде бірқатар маңызды кемшіліктер бар, мысалы: пайдаланушы құпия сөзін басқа адамға бере алады; пароль әлсіз болуы мүмкін, яғни оңай табуға болады; пароль ұсталуы мүмкін. Қашықтан қол жеткізу үшін қарапайым құпия сөздерді пайдалану рұқсатсыз кіру қаупін едәуір арттырады. Пароль аутентификациясының негізгі мәселесі – көптеген пайдаланушылар ұзақ кездейсоқ парольдерді өз басында сақтай алмауында. Сондықтан, әдетте, 5-8 таңбадан тұратын парольдер қолданылады [7].

Нәтижелер. Бұл мақалада қазіргі биометриялық аутентификация жүйелерінің сипаттамалары талданады. Биометриялық жүйелердің тиімділігін бағалау ерекшеліктері қарастырылды. Саусақ іздерінің сынақ деректер базасын құру кезінде синтезделген саусақ іздерін пайдалану алгоритм сапасының нақты суретін алуға мүмкіндік бермейтіні ескерілді. Биометриялық аутентификация технологиялары мен заманауи ақпараттық қауіпсіздік жүйелеріне шолу жүргізілді. Қазіргі заманғы биометриялық технологияларды дамытудың тенденциялары және оларды ақпараттық қауіпсіздікте қолдануы анықталды.

Литература

1. T.Zh. Mazakov, Sh.A. Jomartova, G.Z. Ziyatbekova, T.S. Shormanov, B.S. Amirkhanov, P. Kisala. The image processing algorithms for biometric identification by fingerprints // News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences, 2020. – Vol. 1, – No 439. – P. 14-22. ISSN 2518-170X (Online), ISSN 2224-5278 (Print). https://doi.org/10.32014/2020.2518-170X.2

2. Вакуленко А. Биометрические методы идентификации личности: обоснованный выбор и внедрение / А. Вакуленко, А. Юхин. – М.: Наука, 2007. – 224 с.

3. Зиятдинов А.И. Принципы построения систем биометрической аутентификации / А.И. Зиятдинов. – М.: МФТИ, 2005. – 188 с.

4. Байрбекова Г.С., Нугманова С.А., Мазаков Т.Ж. О тенденции и развитии современных биометрических технологий. Вестник КазНПУ им. Абая, серия физико-математические науки, №1(49), 2015. –С. 198-202.

5. Ларина Е.А., Глушко А.А. Сканирующие методы получения отпечатков пальцев // Молодой ученый. – 2016. – №27. – С. 97-107.

6. Soweon Yoon and Anil K. Jain: «Longitudinal study of fingerprint recognition» PNAS 8555-8560, 2015.

7. М.С. Әлиасқар, Т.С. Шорманов, О.Ж. Мамырбаев, Н.Т. Исимов. Применение биометрического сканера для идентификации человека по отпечаткам пальцев // Вестник КазУТБ. – Нур-Султан, 2019. – №3. – С. 18-22.

References

1. T.Zh. Mazakov, Sh.A. Jomartova, G.Z. Ziyatbekova, T.S. Shormanov, B.S. Amirkhanov, P. Kisala. The image processing algorithms for biometric identification by fingerprints // News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences, 2020. – Vol. 1, – No 439. – P. 14-22. ISSN 2518-170X (Online), ISSN 2224-5278 (Print). https://doi.org/10.32014/2020.2518-170X.2

2.Vakulenko A. Biometricheskie metody identifikacii lichnosti: obosnovannyj vybor i vnedrenie / A. Vakulenko, A. YUhin. – M.: Nauka, 2007. – 224 s.

3. Ziyatdinov A.I. Principy postroeniya sistem biometricheskoj autentifikacii / A.I. Ziyatdinov. – M.: MFTI, 2005. – 188 s.

4. Bajrbekova G.S., Nugmanova S.A., Mazakov T.ZH. O tendencii i razvitii sovremennyh biometricheskih tekhnologij. Vestnik KazNPU im. Abaya, seriya fiziko-matematicheskie nauki, №1(49), 2015. –S. 198-202.

5. Larina E.A., Glushko A.A. Skaniruyushchie metody polucheniya otpechatkov pal’cev // Molodoj uchenyj. – 2016. – №27. – S. 97-107.

6. Soweon Yoon and Anil K. Jain: «Longitudinal study of fingerprint recognition» PNAS 8555-8560, 2015.

7. M.S. Әliaskar, T.S. SHormanov, O.ZH. Mamyrbaev, N.T. Isimov. Primenenie biometricheskogo skanera dlya identifikacii cheloveka po otpechatkam pal’cev // Vestnik KazUTB. – Nur-Sultan, 2019. – №3. – S. 18-22.