УДК
МРНТИ

Сопоставительное исследование методов биометрической идентификации личности

Маликова Феруза Омирзаковна[1,2], Сагинаева Айгерим Кыдыркызы[1], Жанат Нұржан Жанатұлы[1]
Казахский Национальный Университет имени Аль-Фараби[1], Алматинский Университет Энергетики и Связи[2], Алматы, Казахстан
E-mail: feruza-malikova@mail.ru, saginaeva.aigerim@mail.ru, nurzhan_21_04@mail.ru

Аннотация: *При доступе к корпоративным сетям и информационным системам общего пользования предусматривается достоверность идентификации личности. Анализируется правильность идентификации, выполненной с использованием различных технологий, в том числе с использованием биометрии. Приводится обзор наиболее известных способов и технических решений биометрической идентификации. Относительно биометрических идентификаторов применения традиционных технологий с использованием самых используемых искренностью, что достоверность идентификации личности. Разработаны рекомендации по применению определенных технологий биометрической идентификации для подсистем. Использование биометрии для систем с большим количеством зарегистрированных пользователей вызывает сомнение не высокая точность идентификации и большая стоимость. Для широких типов систем биометрическая идентификация пригодна для применения в качестве усиления защиты или в качестве специальных устройств, работающих на территории контролируемого периметра.*

Ключевые слова: *биометрия,идентификация, аутентификация, идентификация личности, анализ, метод.*

Comparative research of methods biometric identification of the personality

Malikova Feruza[1,2], Saginayeva Aigerim[1], Zhanat Nurzhan[1]
KazNU named after Al-Farabi[1], Almaty University of Energy and Communications[2], Almaty, Kazakhstan
E-mail: feruza-malikova@mail.ru, saginaeva.aigerim@mail.ru, nurzhan_21_04@mail.ru

Abstract: *The reliability of identification of the personality at access to corporate networks and public information systems is considered. The reliability of the identification executed with use of different technologies, including with application of biometrics is analyzed. The review of the most known ways and technical solutions of biometric identification is provided. It is shown that the reliability of biometric identification of the personality with use of the most used technologies is comparable with reliability of application of traditional identifiers. Recommendations about use of certain technologies of biometric identification for small systems are developed. For systems with a large number of the registered users the applicability of biometrics raises doubts because of the low accuracy of identification and big cost. For a wide class of systems biometric identification is suitable for use as strengthening of protection or as the special devices working at the territory of controlled perimeter.*
Keywords: *biometrics, identification, authentication, identification of the personality, analysis, method.*

Тұлғаны биометриялық идентификациялаудың әдістерін салыстырмалы түрде зерттеу

Маликова Феруза Омирзаковна[1,2], Сагинаева Айгерим Кыдыркызы[1], Жанат Нұржан Жанатұлы[1]

Әл-Фараби атындағы Қазақ Ұлттық Университеті[1], Алматы Энергетика және Байланыс Университеті[2], Алматы, Қазақстан
E-mail: feruza-malikova@mail.ru, saginaeva.aigerim@mail.ru, nurzhan_21_04@mail.ru

Аннотация: *Корпоративтік желілер мен жалпы пайдаланыстағы ақпараттық жүйелерге қол жеткізу кезінде жеке тұлғаны идентификациялаудың шынайылығы қарастырылады. Әр түрлі технологияларды пайдалана отырып, оның ішінде биометрияны қолдана отырып орындалған идентификацияның дұрыстығы талданады. Биометриялық идентификациялаудың ең танымал тәсілдері мен техникалық шешімдеріне шолу келтіріледі. Ең көп қолданылатын технологияларды пайдалана отырып тұлғаны биометриялық идентификациялаудың шынайылығы дәстүрлі идентификаторларды қолданудың шынайылығымен салыстырмалы екендігі көрсетілген. Шағын жүйелер үшін биометриялық идентификацияның белгілі бір технологияларын қолдану бойынша ұсыныстар әзірленді. Тіркелген қолданушылар саны көп жүйелер үшін биометрияны пайдалану идентификацияның жоғары емес дәлдігі және үлкен құны күмән келтіреді. Жүйелердің кең түрлері үшін биометриялық идентификация қорғауды күшейту ретінде немесе бақыланатын периметр аумағында жұмыс істейтін арнайы құрылғылар ретінде (қол жеткізуді басқару және бақылау жүйесінің бір бөлігі ретінде) пайдалануға жарамды.*

Кілттік сөздер*: биометрия, идентификация,аутентификация, тұлғаны идентификациялау, талдау, әдіс.*

Кіріспе

Соңғы уақытта тұлғаны идентификациялау үшін биометриялық параметрлерді пайдалануға деген қызығушылық үнемі өсуде. Биометрия саласындағы теориялық әзірлемелер заманауи қауіпсіздікті қамтамасыз ету жүйелеріне – дербес компьютердегі ақпаратты қорғаудан биометриялық паспорт және күштің мекемелердің ақпараттық-аналитикалық кешендері сияқты мемлекеттік қосымшаларға дейін енгізіледі. Биометриялық қосымшалар мен жүйелердің саны ұлғаюда. Бұл биометриялық идентификацияға қолданбалы қызығушылықпен де, биометриялық технологиялар саласындағы аппараттық құралдардың және стандарттаудың дамуымен де байланысты [1].

Қоғамды ақпараттандырудың қарқындауына, бұлтты есептеулерге көшуге және осы процестерге федералдық және муниципалдық мемлекеттік органдардың, кәсіпорындардың, ұйымдар мен азаматтардың тартылуына байланысты электрондық өзара іс-қимылға қатысушыларды дұрыс идентификациялау және аутентификациялау мәселелері өзекті болып табылады. Ашық ақпаратты және әртүрлі деңгейдегі шектеулі қол жеткізу ақпаратын қамтитын ақпараттық жүйелерді дамыту және жаңғырту, сондай-ақ олардың неғұрлым тығыз өзара іс-қимылының қажеттілігі пайдаланушылардың ақпараттық ресурстарға, оның ішінде құпия ақпаратты қамтитын қорғалған авторизацияланған қол жеткізуін ұйымдастырудың бірінші кезектегі міндеттерінің біріне қояды. Заңға сәйкес, азаматтың денсаулығының жай-күйі туралы ақпарат құпия ақпараттың ашылуына аса сезімтал түрлерінің бірі болып табылады. Пайдаланушы қол жеткізуін бақылау дұрыс идентификациялау және аутентификациялау міндеттерінсіз мүмкін емес [2]. Мемлекеттік және муниципалдық қызметтер, электрондық сауда, қашықтықтан банктік қызмет көрсету және білім беру, сондай-ақ электрондық денсаулық сақтау жүйесінінің дамуы жеке тұлғаны идентификациялаудың нақтылығы туралы белгілі бір сеніммен айтуға мүмкіндік беретін қашықтықтан электрондық өзара іс-қимыл тараптарын анықтаудың сенімді әдістерін жасауды және іс жүзінде қолдануды талап етеді. Соңғы жылдары ең қарқынды дамып келе жатқан жеке тұлғаны идентификациялау және аутентификациялау әдістерінің бірі биометриялық сипаттамалар бойынша идентификациялау болып табылады. Биометрия пайдаланушыға идентификациялық және аутентификациялық ақпаратты жазудың немесе есте сақтаудың қажет емес деп әзірлеушілерді тартады. Соңғы екі онжылдықта бірнеше

ондаған идентификация әдісі әзірленді. Маркетингтік ақпараттарда өндірушілер идентификациялау дәлдігі туралы өте тартымды деректерді ұсынады, бірақ іс жүзінде бұл деректер жоғары бағаланады. Бұл жұмыста идентификациялаудың кейбір сол қолданылатын әдістерінің шынайылығы қарастырылады, идентификациялаудың ең көп қолданылатын биометриялық тәсілдеріне шолу және қысқаша талдау келтіріледі.

Заманауи жағдайларда тұлғаны идентификациялаудың шынайылық мәселесі

Идентификацияның шынайылығы бойынша пайдаланушы туралы идентификациялау ақпаратының толықтығы мен дәлдігін түсінеміз.

Идентификацияның шынайылығы ақпараттық жүйелерде идентификациялық және аутентификациялық ақпарат туындаған кезде, сондай-ақ оларды сақтау, беру және өңдеу кезінде қателердің туындау ықтималдығына кері пропорционалды. Басқаша айтқанда, идентификацияның шынайылығы тұлғаны идентификациялау процесінің сенімділігімен [3-5] және қатесіздігімен анықталады.

Өзара іс-қимыл тараптарын идентификацияның шынайылық мәселелеріне әлі де тиісті көңіл бөлінбеген, тек қазір көптеген жабық корпоративтік жүйелерге Web-қол жеткізу және басқа ақпараттық жүйелермен алмасу талаптарын қоя бастағандығынан болуы мүмкін. Бұл ретте негізгі мәселе шағын ақпараттық жүйелер үшін де, сондай-ақ ортақ пайдаланылатын ақпараттық жүйелер үшін де идентификация нәтижелеріне белгілі бір сенімділік дәрежесімен сенуге мүмкіндік беретін технологияларды, тетіктерді және идентификация құралдарын айқындау болып табылады. Міндет отандық нормативтік базаның идентификация және аутентификация процестерін орындау қауіпсіздігіне, сенімділігіне және сапасына қойылатын талаптарды қамтымауымен күрделене түседі [6]. Қандай да бір технологияларды, тетіктерді және идентификация құралдарын таңдау мәселелері ақпараттық жүйелердің иелеріне кері қайтаруға берілген. Қауіпсіздік, сенімділік және сапа талаптарына жауап беретін және нарықтағы барлық қолданыстағы және болашағы бар шешімдерді қамтитын таңдау өлшемдерін табу талап етіледі.

Мәселені шешудің ықтимал тәсілдерінің бірі ретінде қашықтан электрондық өзара іс-қимыл қатысушыларын идентификациялау үшін электрондық қолтаңбаны тексеру сертификаттардың кілтін пайдалану қарастырылады, оның тікелей мақсаты басқаларды және иеленушіні идентификациялау функциясы болып табылады. Алайда жұмыста келтірілген электрондық қолтаңбаны тексеру кілтінің сертификаттар иесінің D тұлғасын идентификациялаудың шынайлығын зерттеу мынадай формула бойынша есептелетін шынайылықтың тым төмен мәнін көрсетті:

$$\boldsymbol{D = 1 - \prod_{i=1}^{k} p_i},$$

мұндағы $p_i - i$-ші идентификаторды көрсеткен кезде идентификация қателігінің болмау ықтималдығы. Жеке тұлғаның электрондық қолтаңбаны тексеру кілтінің сертификатының қолданыстағы талаптарына сәйкес міндетті түрде жеке дербес шоттың аты – жөні мен сақтандыру нөмірі болады, бұл электрондық қолтаңбаны тексеру кілтінің сертификатының иесін жалпы қолданыстағы ақпараттық жүйесін бір мәнді идентификациялау үшін анық жеткіліксіз; электрондық қолтаңбаны тексеру кілтінің сертификат иесін заңды тұлғаның қызметкерін идентификациялаумен іс сәл жақсырақ болады, бірақ электрондық қолтаңбаны тексеру кілтінің сертификаты берілген өрістері бойынша оны идентификациялау кезінде иесінің бірегейлік мәселесін шешпейді, себебі идентификация дәлдігі 10^{-4}- тен аспайды. Пайдаланушылар саны 10^5-10^7 құрайтын жалпы қолданыстағы ақпараттық жүйелер үшін 10^{-8}-ретті идентификацияның дәлдігін қамтамасыз ететін сенімді идентификациялау тетіктері болуы қажет. Пайдаланушылардың саны ұлғайған кезде дәлдік тәртібі 10^{-n-1} ретінде бағаланады, мұнда n −жүйені пайдаланушылардың саны. Нарық ұсынатын биометриялық идентификациялау әдістерінің жарамдылығын анықтау үшін дербес идентификатор ретінде идентификацияның шынайылық есебінің жалпы шешімін қарастырамыз.

Идентификация нәтижелері (пайдаланушының тіркелу кезінде дерекқорға енгізілген мәнмен идентификатордың ұсынылған мәнін салыстыру) өзінің табиғаты бойынша ықтималдық теориясының көмегімен зерттеу пәні болып табылуы тиіс. Сондықтан идентификация (ықтималдық сипаттама) және аутентификация (сенімділігі мен сапасы да ықтималдық сипаттама болып табылады) нәтижелеріне сенімділік деңгейін енгізу ұсынылады. Тапсырманы жеңілдету үшін идентификацияның 2 деңгейін енгізуге болады: оңайлатылған және стандартты, және аутентификацияның 3 деңгейін: қарапайым, күшейтілген және қатаң. Мұндай тәсіл идентификация мен аутентификация тәуекелдерін талдау негізінде жүргізілген идентификация мен аутентификация үдерістері мен нәтижелерін зерттеумен және сенімділікті талдаумен келісіледі [7].

Субъект ақпараттық жүйелерде алғаш рет жүгінген (жаңа пайдаланушыны тіркеген) кезде бірегейлендірудің шынайылығын және қайталама (жиі қайталанған) өтініштер кезінде бірегейлендірудің шынайылығын ажырату керек.

Бұл ретте, өтініш беруші алғаш рет жүгінген кезде жеке басын идентификацияның шынайылығы мынадай аспектілерге байланысты екенін ескеру қажет:

- идентификацияның сапасы – ұсынылған идентификаторларды тіркеу кезінде базаға енгізілген деректермен салыстыру жолымен бір субъектінің екіншісінен айырмашылығы;
- идентификация процесінде бірінші (қаскүнем заңды user ретінде идентификацияланған) және екінші түрдегі (заңды пайдаланушы идентификацияланбаған) қателер болады;
- идентификаторлар санына және ең бастысы, салыстыру механизмдерінің сенімділігі мен қауіпсіздігіне байланысты салыстыру нәтижелеріне сенімділік деңгейін енгізу қажеттілігі;
- даулы жағдайларды талдау үшін мемлекеттік дерекқордан идентификаторлардың сәйкестігін растау үшін процестердің нәтижелерін тіркеу қажеттілігі.

Қайталама идентификация кезінде (ақпараттық жүйенің ресурстарына қайта жүгінулер) идентификация процесі үміткер ұсынған идентификаторларды тіркеу кезінде ақпараттық базаға бұрын енгізілген деректермен салыстыру рәсіміне жинақталады. Қарапайым жағдайда бұл бір идентификатор (мысалы, логин) болуы мүмкін, неғұрлым күрделі идентификация схемаларында бұл жүйемен берілген идентификаторлар санын көрсету процедурасы болуы мүмкін. Мысалы, азамат мемлекеттік қызмет порталына алғашқы рет жүгінген кезде кем дегенде паспорттың нөмірін және жеке дербес шоттың сақтандыру нөмірін көрсету қажет.

Өзекті мәселелердің бірі куәландырушы орталыққа электрондық қолтаңбаны, білікті электрондық қолтаңбаны тексеру кілтінің сертификатына алғаш рет жүгінген өтініш берушіні бастапқы идентификация процесін реттеудің жеткіліксіздігі болып табылады. Ақпараттандыру процесіне мемлекеттік және муниципалдық қызметтерді тартудың объективті қажеттілігі, бір жағынан тәуекел операциялары аз үшін оңайлатылған идентификацияны жүргізу мүмкіндігі туралы ережені – екінші жағынан одан әрі жүгінулер кезінде идентификацияның нақтылық деңгейін одан әрі арттыра отырып, мемлекеттік қызметтердің бірыңғай порталын пайдаланушыларды жеңілдетілген идентификация мүмкіндігіне жол береді. Пайдаланушы жүргізетін операциялар тәуекелдерінің деңгейіне байланысты оңайлатылған идентификациядан бастап (ұялы телефон нөмірі, электрондық пошта мекенжайы бойынша), стандартты идентификация (сенімсіз куәландырушы орталық берген тексеру кілті сертификатын көрсету немесе өтініш берушінің куәландырушы орталықтың тіркеу орталығына жеке келуі) және күшейтілген идентификацияға дейін идентификация тәсілдерін бөлеміз. Идентификаторлар:

1. Электрондық поштаның адресі
2. Ұялы телефонның нөмірі
3. ЭҮ біліктілік сертификаты
4. Жеке өтініші

Идентификацияның бастапқы деңгейі, төменгі тәуекелдер

Идентификацияның стандартты деңгейі, орташа тәуекелдер

5. Паспортты түпнұсқалыққа тексеру
6. Екі құжатты түпнұсқалыққа тексеру
7. Жеке шоттың сақтандыру нөмірі, ЖСН
8. Веб-камераға суретке түсіру
9. Биометрияны тексеру

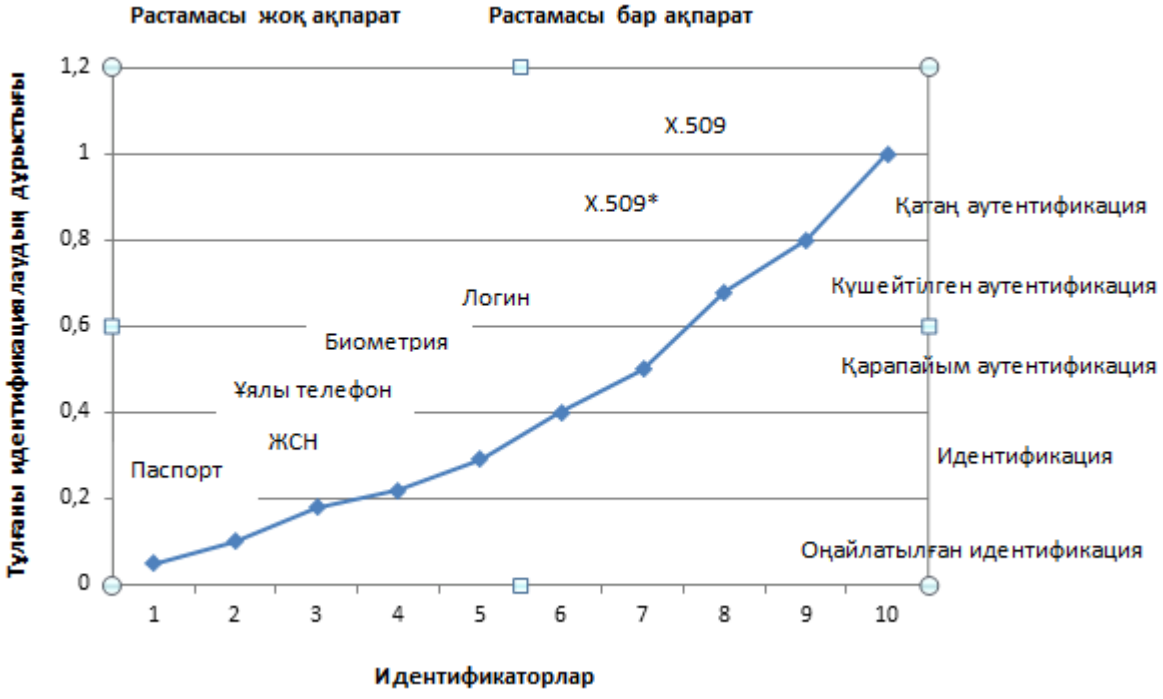
} Идентификацияныңкүшейтілген деңгейі, жоғары тәуекелді операциялар

Бастапқы айналым кезінде болжанатын операциялар тәуекелдерінің деңгейіне байланысты идентификацияның шынайылығы жоғарда көрсетілді.

Электрондық пошта арқылы жіберілген сканерленген паспортқа қарағанда өтініш берушінің тіркеу орталығына жеке келуі ЖСН және жеке дербес шоттың сақтандыру нөмірін тексеру, сондай-ақ паспорттағы фотосуретті ұсынушының тұлғасымен салыстыру арқылы идентификацияның дұрыстығын едәуір арттыруы мүмкін; бұл ретте паспорттың түпнұсқалығын бірқатар ірі банктер мен федералдық құрылымдарда қабылданған рәсімдер арқылы тексерген жағдайда идентификацияның дұрыстығы неғұрлым жоғары деңгейге көтеріле алады.

Аутентификацияның дұрыстығы, сондай-ақ пайдаланушының электрондық қол қою рәсімін тудыратын қолданбалы бағдарламалық қамтамасыз етуге қол жеткізуін басқару үшін де, құжатқа немесе хабарламаға қол қою кезінде электрондық қол қою құралы иесінің еркін білдіру рәсімін ұйымдастыру үшін де маңызды.

Жоғарыда ұсынылған қарапайым аутентификация деңгейлері түпнұсқалықты растау технологиялары мен қолданылған тетіктерге байланысты төменгі деңгейлерге бөлінуі мүмкін. Іс жүзінде бұл деңгейлер шабуылдаушының заңды қолданушының атымен авторизациялау қауіптерімен байланысты. Батыстың ережелері мен стандарттарында пайдаланылатын «идентификация» термині идентификацияны және аутентификацияны қамтиды. Мұндай жалпылама тәсіл терминдеріндегі идентификацияның дұрыстығын бағалау, мысалы 1-суретте көрсетілген. Осы суретте көрсетілген кейбір нүктелерді қарастырайық.

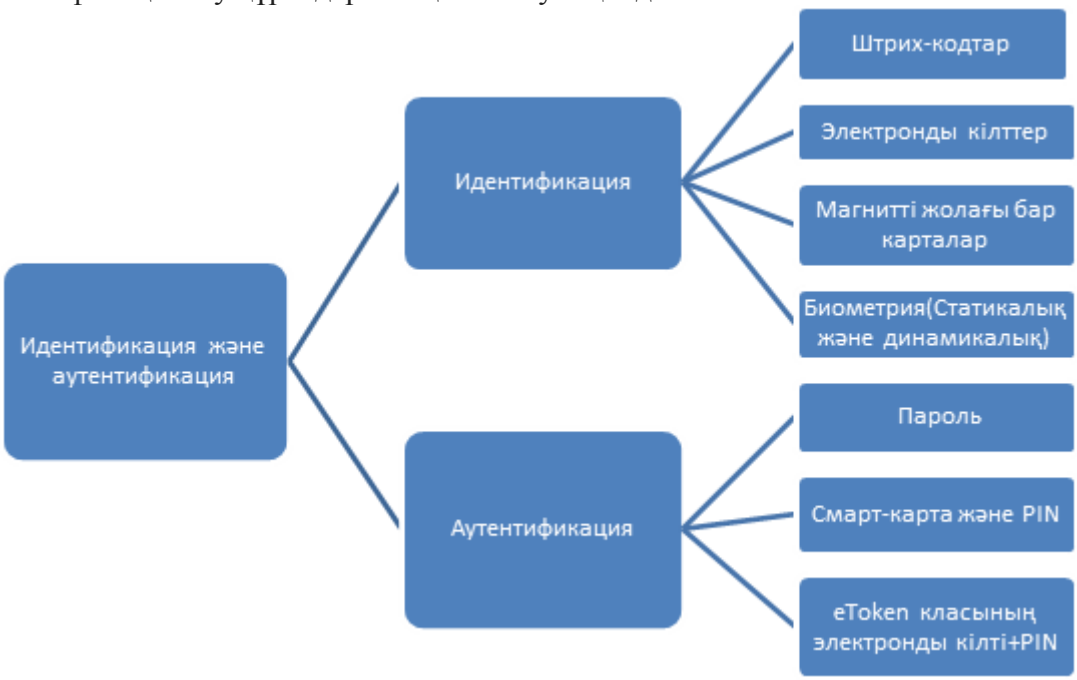


1-сурет. Тұлғаны идентификациялау және аутентификациялау деңгейлері.

Мысалы, паспорттық деректерді қашықтық режимде (паспорт беттерін сканерлеу) ұсыну оңайлатылған идентификацияны жүргізу үшін негіз бола алады. Жоғарыда сипатталған паспорттың сканерленгенін көрсету емес, жеке өзі келген кезде паспорттың өзін көрсету және оның түпнұсқалығын тексеру идентификация деңгейін айтарлықтай арттырады. Егер идентификациялау пунктінде паспортты тексеру кезінде жауапты тек оның

иесі білетін сұрақтар қойылса,онда бұл идентификация емес, иесінің аутентификациясы болар еді. Келесі нүкте өтініш берушінің оның биометриялық ақпаратын беруі болып табылады. Биометрияны қолдану паспортты немесе ЖСН-нің ұрланған деректерін және жеке дербес шоттың сақтандыру нөмірін сапалы қолдан жасау мүмкіндігіне қарағанда антропологиялық деректерді бірнеше жағдайларда қолдан жасау қиын. Мұндай жағдайларда идентификацияның дұрыстығы идентификация процесінде пайдаланылатын механизмге және қолданылатын технологияларға байланысты болады. Мысалы, 10^{-10} ретінде бағаланатын ДНҚ талдау әдісінің дәлдігі кезінде салыстырылатын үлгілерді іздеу және сараптамалық талдау жолымен тұлғаны идентификациялаудың жиынтық дәлдігі деректер базасында $10^{-5} - 10^{-4}$шегінде болады [5,8].

Нақты деректер болмаған жағдайда, жаңа шетелдік паспорттардағы биометриялық деректерді пайдалануға болады. Барлық оң пен теріс кезінде биометриялық сипаттамаларды пайдалану әлемдік тренд болып табылады. Өтініш берушінің сол немесе басқа тәсілмен алынған биометриялық деректері одан әрі оны идентификациялау үшін ғана емес, мысалы, қол жеткізу сертификаттары мен электрондық қолтаңбаны тексеру кілтінің сертификаты үшін негізгі ақпараты бар токенді бұғаттаудан шығару үшін пайдаланылуы мүмкін. X. 509* белгісімен белгіленген жоғарғы нүкте (1-сурет) X. 509 нүктесінен ерекшеленеді, бұл жағдайда шығарылмайтын жабық кілтпен SSCD (SecireSignatureCreationDevice – электрондық қолтаңбаның криптографиялық кілттерін қауіпсіз генерациялау құрылғысы) құрылғысы қолданылады. Бұл жағдайда мұндай құрылғы иесінің идентификация және аутентификациясының шынайылығы негізгі ақпараттарды ауыстыру ықтималдығы көп негізгі контейнерлерді сақтауға арналған құрылғыларды қолданғаннан жоғары. Сонымен қатар, биометрия орнын белгілі және кең қолданылатын технологиялармен қатар анықтау үшін 2-суретте ұсынылған қолданылатын технологиялар тұрғысынан идентификациялау және аутентификациялау құралдарының жіктелуін қолданамыз.



2 – сурет. Қолданылатын технологиялар тұрғысынан идентификация және аутентификация құралдарының жіктелуі.

Идентификациялау және аутентификациялау процестерін реттейтін халықаралық нормативтік құжаттардың көптігіне қарамастан, биометриялық белгілер бойынша тұлғаны идентификациялаудың дұрыстығының мәселелері аяғына дейін зерттелмеген. Әдетте идентификация әдістерін салыстыру кезінде идентификация технологиясының дәлдігі ғана қарастырылады. Осы жұмыста осындай тәсілге қарағанда идентификация рәсімі объектінің идентификаторларын бастапқы тіркеу кезінде де, тікелей идентификация процесінде де

мүмкін болатын қателіктер мен қателерді ескере отырып, "Иә/Жоқ" класының шешімін қабылдау процесі түрінде қаралады.

Барлық биометриялық әдістер ықтималдық және статистикалық әдістерге негізделген. Бұл әдіс бірнеше жолмен бағалануы мүмкін, ең көп таралған тәсілде негізгі сипаттамалар ретінде бірінші және екінші түрдегі қателерді қабылдауға болады. Бірінші түрдегі қате (FRR – False Rejection Rate) – қол жеткізуге құқығы бар пайдаланушыға қол жеткізуден жалған бас тарту ықтималдығы. Екінші түрдегі қате (FAR-False Acceptance

Rate) - бұл жүйе бөтен адамды өзі ретінде қате танығанда жалған кіру ықтималдығы. Жүйе жұмысының өлшемдерінің бірі келесі тәсіл болуы мүмкін: жүйе FAR бірдей мәндерінде FRR мәні аз болса, соғұрлым жақсы. Кейде FRR және FAR кестелерінің қиылысу нүктесін анықтайтын EER салыстырмалы сипаттамасы қолданылады. Адамның статикалық биометриялық сипаттамаларын қолданатын негізгі әдістер саусақтардың папиллярлы суреті бойынша, кемірқосақ қабығы бойынша, бет геометриясы, көздің торлы қабығы, қол тамырларының суреті, қол геометриясы бойынша идентификациялау болып табылады. Сондай-ақ динамикалық сипаттамаларды пайдаланатын әдістердің біріккен ұжымы бар: дауыс, қолжазба сызу динамикасы, жүрек ырғағы, жүру бойынша идентификация.

Бұл жұмыста кіруді бақылау және басқару жүйелерінде қолданылатын сипаттамалар ғана қарастырылады, әдетте бұл статикалық сипаттамалар. Мәтінді жазу кезіндегі динамикалық сипаттамалардан тек дауыспен тану статистикалық мәнге ие. 1-кестеде статикалық сипаттамалар бойынша сәйкестендірудің негізгі әдістері келтірілген. [9,8,10,11,12,13].

Тұлғаны идентификациялау құралдарының жіктелуі және негізгі сипаттамалары

[8,12] жұмыста жүйенің сапасын бағалауға мүмкіндік беретін бірнеше эмпирикалық сипаттамалар берілген:

* жасанды төзімділік-биометриялық идентификаторды алдау қаншалықты оңай жалпылайтын эмпирикалық сипаттама;

* қоршаған ортаға тұрақтылық – жарық немесе температураның өзгеруі сияқты әртүрлі сыртқы жағдайларда жүйе жұмысының тұрақтылығын эмпирикалық бағалайтын сипаттама;

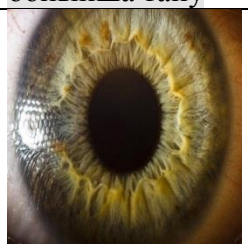
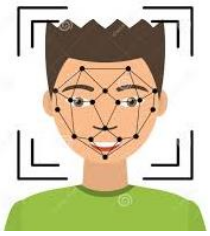
* пайдаланудың қарапайымдылығы-биометриялық сканерді пайдалану қаншалықты қиын екенін жүрісте идентификация мүмкін бе екенін көрсетеді;

* жұмыстың жылдамдығы;

* жүйенің құны.

1-кесте.

Статикалық сипаттамалар бойынша идентификацияның негізгі әдістері.

Биометриялық танулар	Көздің шатырша қабықшасы бойынша тану	Саусақ іздері бойынша тану	Бет бойынша тану	Алақанның тамырлары бойынша тану
Әдістің нысаны				
Әдістеме	Бірнеше суреттің көмегімен көздің шатырша қабықшасының кескінінің	Саусақтардағы папиллярлы өрнектердің суреттерінің әрбір адам үшін бірегейлігі.	Адам тұлғасының үш өлшемді құрылымын талдайды,	Инфрақызыл камера қолды сыртқы немесе ішкі жағынан түсіреді.

	белгілеуі.		деректерді деректер базасына енгізеді және жиналған деректерді пайдалануға мүмкіндік береді.	
Әдістің артықшы-лықтары	Алгоритмнің сенімділігі, нысанды зақымдалудан және көшірмесі болуынан қорғалуы.	Сканерлеу құрылғыларының төмен құны, қарапайым процедуралар.	Сканерлейтін құрылғымен байланысының қажет еместігі.Сыртқы факторларға төмен сезімталдық(сақалдың, көзілдіріктің пайда болуы). Сенімділіктің жоғары деңгейі.	Бұл әдістіңде сканерлейтін құрылғымен байланысудың қажеті жоқ. Жоғары сенімділік.
Әдістің кемшілік-тері	Жоғары баға, дайын шешімдердің төмен қолжетімділігі.	Бас тартудың жоғары дәрежесі, сыртқы әсерлерге тәуелділігі(кесу, күйік), көшірмесі болудың мүмкіндігі.	Қымбаттығы. Мимиканың өзгеруі әдістің статистикалық сенімділігін нашарлатады.	Сканерді күн сәулесімен және галогенді шамдардың сәулелерімен жарықтандыру ға болмайды. Кейбір аурулардың кедергі келтіруі.
Негізгі өндіруші-лер	Samsung, OKI Iris, LG electronics, Panasonic, Apple.	SecBayometric, Apple, Biolink, Digital Persona, Huawei, Samsung.	Genex technologies, Identity Solutions, Apple, Cognitec Systems.	

Бұл жүйелер келесі сипаттамаларға ие болуы керек: бұйымға тұрақтылық, қоршаған ортаға тұрақтылық, пайдаланудың қарапайымдылығы, құны, жылдамдығы, уақыт бойынша биометриялық белгінің тұрақтылығы. FAR және FRR қатынасы жүйенің тиімділігі мен оны пайдаланудың кеңдігін анықтайды. Сонымен қатар, екі қолды біріктіру жолымен, бірақ адаммен жұмыс істеу кезінде кететін уақытты ұлғайту кезінде бірнеше саусақтарды біріктіру және көктамыр бойынша тану жолымен дактилоскопиялық әдіс үшін жүйенің дәлдігін төртбұрышты түрде арттыруға болады. Келтірілген нәтижелерді қорыта келе, орта және үлкен кәсіпорындар үшін, сондай-ақ қауіпсіздікті барынша талап ететін нысандар үшін көздің шатырша қабығын биометриялық қол жеткізу құралы ретінде пайдалану ұсынылады. Бірнеше жүздеген адамға дейін қызметкерлер саны бар нысандар үшін саусақ іздері бойынша қол жеткізу оңтайлы болады. Пайдаланушылардың саны көп ақпараттық жүйе үшін биометрия негізінде қол жеткізу жүйелерін құру экономикалық тұрғыдан ақталмаған.

Мұндай жүйелер үшін қосымша фактор ретінде деректер базасынан биометриялық сипаттамаларды пайдалануға болады.

Биометриялық сәйкестендіруге арналған қауіпсіздік қатері

Биометриялық сәйкестендіру үшін ең танымал қауіпсіздік қатерлерін қарастырайық:

1. Авторизация сервисінен биометриялық ақпаратты ұрлау қаупі. Арнайы әдістермен көрсетіледі, бірақ хештеуден әлдеқайда күрделі. Биометриялық ақпаратты араластырудың жұмысы және арзан аналогы пайда болғанша оны ұрлауға болады. Қазіргі уақытта тіпті құпия сөздер тұрақты емес хештері бар базада жиі сақталады.

2. Желі бойынша берілетін биометриялық ақпаратты ұстап қалу. Байланыс арнасын шифрлеу арқылы көрсетеді. Құпия сөзге қарағанда, электрондық қолтаңбаның көмегімен түпнұсқалығын тексеру арқылы толық шифрлау қажет.

3. Физикалық немесе бағдарламалық бұзылған аутентификация құрылғысынан биометриялық ақпаратты оқу. Құрылғылардың физикалық және бағдарламалық қорғау шаралары арқылы көрсетіледі.

4. Адамнан немесе ақпарат тасымалдаушыдан биометриялық ақпаратты ұрлау. Егер адам қатысты жиһазға, ыдыс-аяққа және т.б. қажетті қол жетімділігі болса, онда саусақ іздерін ұрлауға болады. Адамның сөзін жазып, биометриялық идентификация жүйесі ұқсас деп санайтын дыбыстарды синтездеуге болады. Мәтінді дауыстап оқу жүйесі бар тиісті түзету кезінде оларды бұрмалау үшін пайдалануға болады. Торлы және шатырша тамырларының суретіне қарағанда жақсы: мұнда ақпаратты есептеу қиын. Қауіп қолдан жасаудан ажырата алатын аутентификацияның күрделі жүйелерімен ғана реттеледі. Алайда, булау сенімді емес.

5. Биометриялық ақпаратты әлеуметтік инженерия әдістері немесе жасанды құрылғылар көмегімен оқу. Булау қиын. Екінші жағдайда құрылғыны чиптің қорғалған жадында ақпарат идентификация және аутентификация сертификаты бар чиптермен жабдықтау ұсынылады. Сонда пайдалану алдында құрылғының ақпараттық жүйенің серверімен өзара аутентификациясы жүргізіледі.

6. Құпия сөзге қарағанда, адам аккаунтқа қолжетімділікті шектейтін авариялық құпия сөзді хабарлай алмайды. Адам қалай тырысса да, өзінің биометриялық ақпаратын өзгерте алмайды. Алайда, бір жерде білуге болатын парольге қарағанда алыстан енгізуге болады, биометриялық идентификация биометриялық ақпаратты енгізу үшін адамды талап етеді (кесілген саусақтарды немесе дауысты қолдан жасау, нақтырақ айтқанда көшірме жүйесін қоспағанда). Осылайша, қаскүнем жасырын түрде адамды идентификациядан өтуге мәжбүрлеу қиын болады, бірақ егер оқитын құрылғылар бақыланатын аймақтың аумағында орналасқан болса, арнайы шлюздермен жабдықталған және күзетілетін жағдайда ғана болса. Әйтпесе, қауіп мүлдем көрсетілмейді.

Болашақта жүзеге асатын биометриялық технологиялар

Қауіпсіздік жүйелерінде қолданылуы мүмкін технологиялар саласы үнемі кеңеюде. Бірқатар биометриялық технологиялар әзірлеу сатысында, олардың кейбіреулері өте болашағы бар технологиялар болып саналады. Оларға сәулеленудің инфрақызыл диапазонындағы бет бейнесінің танылуы, ДНҚ сипаттамалары, клавиатуралық жазу, сандық ультрадыбыстық ақпарат (тері спектроскопиясы) негізінде саусақтардағы тері мен эпителий құрылымын талдау, алақандардың іздерін талдау, құлақ раковинасының формалары, адамның жүрісінің сипаттамалары, адамның жеке иістері, көктамырлардың орналасуы бойынша тану технологиялары жатады. Бірнеше үлкен үміт беретін жүйелердің жұмыс сапасын бағалау [12] келтіріледі, ал вариативті шешім қабылдаудың негізділігі ДНҚ талдауы бойынша тұлғаны идентификациялау [13] келтіріледі.

Қорытынды

Идентификацияны талдауға қарастырылған тәсіл биометрияның әр түрлі әдістерінің нақтылығы мен сенімділігін идентификацияның басқа әдістерімен салыстыра отырып бағалауға мүмкіндік береді. Жұмыста көрсетілгендей, биометрияны қолдану пайдаланушылар саны көп жүйелер үшін идентификацияның сенімділік мәселелерін шешпейді, бірақ жүздеген өлшенетін пайдаланушылар саны бар жүйелерге, сондай-ақ физикалық қолжетімділікті бақылау және басқару жүйесінің бір бөлігі немесе аутентификацияның сапалы толтырғыш факторы ретінде өте маңызды жүйелерге қолжетімділікті ұйымдастыру кезінде субъектілерді идентификациялаудың дұрыстығын арттыра алады. Жүргізілген талдау биометриялық идентификация құралдарының тұтастай алғанда өнеркәсіптік дайындығы, сенімділігі мен функционалды тұрақтылығы тым жоғары емес екенін дәлелдейді.Тіркелген пайдаланушылар саны көп жүйелер үшін биометрияның қолданылуы бірдейлендірудің жоғары дәлдігіне және үлкен құнына байланысты күмән тудырады. Жүйенің кең класы үшін биометриялық идентификация қорғауды күшейту ретінде немесе арнайы бөлінген аймақтарда бақыланатын аймақтың аумағында жұмыс істейтін құрылғылар ретінде пайдалануға жарамды.

Пайдаланылған әдебиеттер

1.Ресейлік ақпаратты-коммуникациялы технологиялар саласын дамытудың үміт күтерлік бағыттары (Ұзақ мерзімді технологиялық болжам. Foresight ресейлік АТ). – http://apkit.ru.

2. Грушо А.А., Применко Э.А., Тимонина Е.Е. Компьютерлік қауіпсіздіктің теориялық негіздері – М.: Академия, 2009.

3. Громов Ю.Ю., Иванова О.Г. Ақпараттық жүйелердің сенімділігі/ Тамбов: ГОУ ВПО ТГТУ. 2010.

4. *Шубинский И.Б.* Ақпараттық жүйелердің құрылымдық сенімділігі. Талдау әдістері/ Ульяновск: «Печатный двор» областық типографиясы, 2012.

5. *Шубинский И.Б.* Ақпараттық жүйелердің функционалдық сенімділігі. Талдау әдістері / Ульяновск: «Печатный двор» областық типографиясы, 2012.

6. *Сабанов А.Г.* идентификация және аутентификация бойынша шетелдік нормативтік базаға шолу // Инсайд. Ақпаратты қорғау, 2013. №4(52).

7. *Сабанов А.Г.* Қашықтан аутентификациялаудың сенімділігін зерттеудің әдістері // Электробайланыс, 2012. №10.

8. *S.Soviany, H.Jurian* Биометриялық идентификация жүйелері үшін деректерді біріктіру және жіктеудің иерархиялық моделі.

9. Литвиненко В., Чакчир С. Биометрия / Қауіпсіздіктің алгоритмы, 2006. №3.

10. *Аутентификация*. Теория және тәжірибе. М.: Байланыс желісі-Телеком, 2009.

11. *Смирнова Г.Н., Сорокин А.А., Тельнов Ю.Ф.* Экономикалық ақпараттық жүйелерді жобалау – М.: МЭСИ. 2004. – 452с.

12. Перепечина И.О. Соттық ДНҚ идентификациядағы категориялық сараптаманың қорытындысы және оны шешудің тәсілдері.

13. *Сабанов А.Г.* Идентификация және аутентификация технологияларына шолу // Құжаттамалық телекоммуникация, 2006. №17.