ҒТАМР 20.01.04

Ж.Е. Доумчариева[1] – *негізгі автор*,
М.К. Есеналиева[2]

[1]*Магистр, аға оқытушы,* [2]*Магистр, оқытушы*

[1]*https://orcid.org/0009-0006-4085-8409* [2]*https://orcid.org/0000-0002-9240-5579*

[1]*М.Х. Дулати атындағы Тараз өңірлік университеті,*

Тараз қ., Қазақстан Республикасы

[1]zhanagul78@mail.ru

https://doi.org/10.55956/VJYW8091

МОБИЛЬДІ ҚҰРЫЛҒЫЛАРДА АУТЕНТИФИКАЦИЯЛАУДЫҢ БИОМЕТРИЯЛЫҚ ӘДІСТЕРІ

Аңдатпа. Мақалада "Биометриялық аутентификация" ұғымы қарастырылады, биометриялық аутентификацияның әртүрлі заманауи мүмкіндіктері, аутентификациялаудың биометриялық әдістері, олардың қалай қолданылатыны, сондай-ақ олардың артықшылықтары мен кемшіліктері баяндалады. Мобильді құрылғылар қазіргі қоғамда маңызды орын тапты, олардың жүздеген миллиондары қолданылуда. Смартфондар сияқты мобильді құрылғыларда сенімді және бейтарап пайдалануды сәйкестендіру және аутентификация бүгінгі таңда өзекті мәселелер. Осы саладағы заманауи шешімдердің көпшілігі «құрылғы құлпын ашу» сценарийіне негізделген – смартфон құлпын ашу үшін пайдаланушы берген ақпаратты (аутентификация факторларын) тексеру. Олардың көпшілігі құпия сөздер мен PIN кодтарына негізделген әлсіз аутентификация механизмдерін пайдаланады, олар оңай бұзылып, осылайша шабуылдаушыларға құрылғыға және оның сақталған деректеріне қол жеткізуге мүмкіндік береді. Сондықтан күшті аутентификацияға қажеттілік артып отыр және әртүрлі биометрияны мобильді платформаға қолдану маңызы артуда.

Тірек сөздер: биометриялық аутентификация, саусақ ізі, пайдаланушы, тор көзі, тану, сканерлеу, мобильді құрылғылар.

Доумчариева, Ж.Е. Мобильді құрылғыларда аутентификациялаудың биометриялық әдістері [Мәтін] / Ж.Е. Доумчариева, М.К. Есеналиева // Механика және технологиялар / Ғылыми журнал. – 2024. – №1(83). – Б.205-213. https://doi.org/10.55956/VJYW8091

Кіріспе. Уақыт өте келе әр нәрсе өзгеріске ұшырайды. Бүгінде биометриялық жүйелер барлығына таныс және 2020 жылдан бастап биометриялық аутентификация күнделікті өмірде қолданыла бастады. Биометрия адамның бірегей сипаттамаларына негізделген және әдетте физиологиялық және мінез-құлық деп екі санатқа бөлінеді. Физиологиялық биометрия – бұл адамның саусақ іздері, беті және қолы сияқты физикалық белгілеріне қарай жіктеуге негізделген. Мінез-құлық биометриясы адамның ерекше мінез-құлқына, мысалы, дауысына және қолтаңбасын жазу тәсіліне сүйенеді. Биометриканың барлығы биометриялық үлгіні белгілі үлгімен салыстыру негізінде жұмыс істейді, ол жүйеге алғаш тіркелген кезде пайдаланушыдан қауіпсіз түрде алынады.

Биометрия парольдерді аутентификацияның қарапайым және қауіпсіз әдісі ретінде ауыстырады. Биометриялық аутентификация (метрика) пайдаланушының биологиясын (мысалы, бас бармақ ізі) осы метриканың сақталған нұсқасы бойынша өлшейді. Егер сәйкестік анықталса, авторизация бірден беріледі. Биологияға негізделген дәлелдеу біз көрген кез-келген басқа аутентификация технологиясына қарағанда қауіпсіз болғандықтан және оның жылдамдығы, дәлдігі және қолжетімділігі арқасында биометриялық аутентификация әдеттегі жағдайға айналуда [1].

Биометриялық жүйелердің *маңыздылығы* дәстүрлі жүйедегідей кілтті беру мүмкіндігі жоқ жеке тұлғаны сәйкестендіруге бейімделгендігінде және пайдаланушының көзқарасы бойынша көптеген жағынан ыңғайлы болуында.

Биометриялық сканерлерді физикалық кіру нүктелерінің қауіпсіздігін қамтамасыз ету үшін пайдалануға болады. Дүние жүзіндегі үкіметтер әуежайлардың шығысында және Ұлттық шекараларда саусақ іздері мен торлы қабық сканерлерін қолданып жатыр. Жеке компаниялар биомаркерлер мен нысандарға қолжетімділікті шектеу арқылы құпия ақпаратты қорғайды.

Бірақ биометриялық технологияның кең таралуына ықпал еткен нәрсе – оны смартфондарға, планшеттерге және ноутбуктерге – пайдаланушы интерфейсі (UI) бар кез-келген сандық құрылғыларға біріктіру.

Биологиялық аутентификация танымал болуда, өйткені ол талғампаз, тиімді әрі қауіпсіз, және оның айналасындағы кедергілер жойылды. Биометриялық оқырмандар жадпен (парольдермен) немесе деректерді шығарумен (2FA/MFA) жұмыс жасамай-ақ бір қадамдық қол жетімділікті қамтамасыз етеді.

Зерттеу шарттары мен әдістері. Аутентификация әдістері ретінде биометриялық идентификаторлардың қандай түрлері қолданылады?

Биометрия екі түрге бөлінеді: физиологиялық және мінез-құлық. Енді осыларға жеке тоқталайық.

Адамның жеке басын растау үшін қолдануға болатын физиологиялық биометрия:

- саусақ ізін сканерлеу;
- бетті тану;
- көзді сканерлеу.

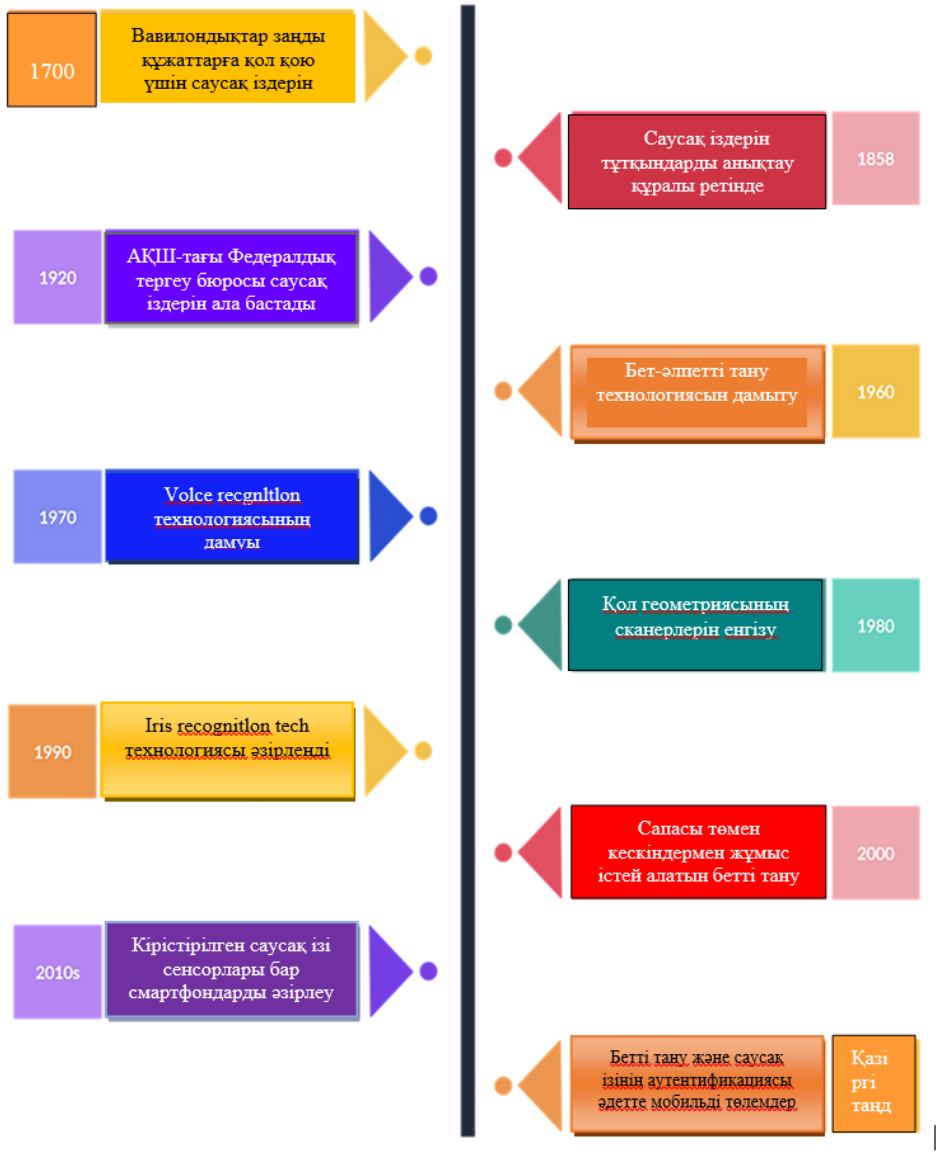
Мінез-құлық биометриясы:

- дауысты тану;
- қолтаңбаны тану.

2000 жылдары сапасы төмен суреттермен және бақыланбайтын орталарда жұмыс істей алатын бетті тану технологиясы жасалды. Бұл қауіпсіздік пен бақылау қолданбаларында осы технологияның кеңінен қолданылуына әкелді [2].

2010 жылдардың ортасында саусақ ізі сенсорлары бар смартфондардың дамуы мобильді құрылғыларға биометриялық аутентификацияны енгізудің өсуіне әкелді. Бүгінде бет-әлпетті тану және саусақ ізінің аутентификациясы мобильді төлемдер мен құрылғы құлпын ашу үшін кеңінен қолданылады.

Соңғы жылдары биометриялық аутентификация физикалық сипаттамалар шеңберінен шығып, теру үлгілері мен тінтуірдің қозғалысы сияқты мінез-құлық сипаттамаларын қамтиды. Мінез-құлық биометриясы деп аталатын бұл технологиялар онлайн-банкинг пен электрондық коммерциядағы алаяқтық пен аутентификацияны анықтау үшін қолданылады. Биометриялық аутентификацияның даму кезеңдері 1-суретте берілген.



Сурет 1. Биометриялық аутентификацияның даму кезеңдері [1]

Биометриялық аутентификация біздің өмірімізге жасырын түрде енеді. Біз биометрияны тек фантастикалық фильмдерден көріп келген едік, ал бүгін смартфонның құлпын саусақ ізімен, бетті сканерлеумен немесе тіпті көзбен ашамыз.

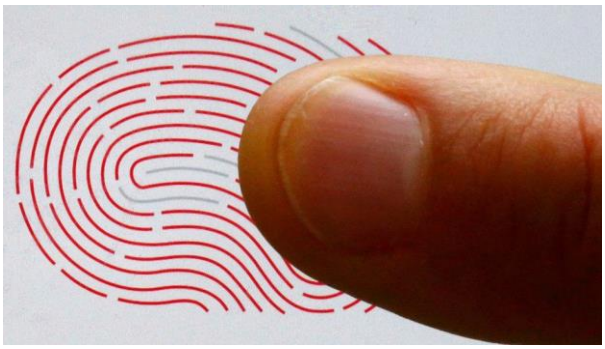
Биометриялық аутентификация – пайдаланушының биометриялық бейнесін ұсыну және оны алдын ала жасалған аутентификация хаттамасына сәйкес түрлендіру арқылы пайдаланушының жарияланған атының түпнұсқалығы мен дәлелін тексеру процедурасы. Ол Match-on-Card архитектурасына негізделген (карта бойынша есептеу). Бұл архитектура смартфонның қауіпсіз аймағында тікелей қол жеткізу немесе бас тарту туралы шешім қабылдауға қабілетті, өйткені смартфонда сандық саусақ ізі үлгілері сақталады.

Зерттеу нәтижелері. ***Физикалық биометрия түрлері.***

Саусақ ізінің аутентификациясы. Қолданушыны сәйкестендіру құралы ретінде саусақ ізі басқа құралдарға қарағанда заманауи мобильді құрылғыларда кеңінен қолданылады.

Кез келген саусақ ізі сканерінің екі функциясы бар: саусақ ізінің кескінін алу және оның үлгісін дерекқордағы басқа үлгілермен салыстыру (2-сурет). Заманауи смартфондар келесі саусақ ізі сканерлерін пайдаланады:

- сыйымдылық – саусақтарымыздан келетін электрлік сигналдарды өлшеу. Баспаның көтерілген бөлігі мен оның депрессиясы арасындағы сыйымдылық айырмашылығын талдау, содан кейін баспаның «картасы» қалыптасады және түпнұсқамен салыстырылады;
- ультрадыбыстық – саусаққа жіберілетін, шағылысқан және өңделетін дыбыс толқындарының көмегімен саусақтың бетін сканерлеу;
- оптикалық – саусақ ізін суретке түсіру және сәйкестікке салыстыруды орындау [2].



Сурет 2. Саусақ ізін тану

Негізгі артықшылығы – бұл сәйкестендіру әдісінің қауіпсіздігі, өйткені әр адамның саусақ ізі ерекше, сондықтан шабуылдаушылар оны қолдан жасай алмайды.

Кемшіліктердің ішінен сканердің әртүрлі жағдайларда дұрыс жұмыс істеуін ажыратуға болады: дымқыл саусақ іздерін нашар анықтау, тыртықтар мен сызаттардың болуы тану сапасына да әсер етеді, сонымен қатар көптеген сканерлер құйманы нақты саусақтан ажыратпайды және бұл қазірдің өзінде қауіп төндіреді.

Саусақ ізі сканерлері смартфондарға енгізілген алғашқы биологиялық оқу тәсілі болды, Apple және Samsung осы бағытта көш бастады. Содан кейін Apple iPhone X телефонында бет-әлпетті тану мүмкіндігін шығару арқылы бір қадам алға басты. Смартфон пайдаланушылары өз өмірін басқаратын жүздеген қолданбаларға жылдам қол жеткізу үшін экрандарын түрту немесе қарау мүмкіндігін пайдаланды. Бірақ жаңа биосканерлер саусақ іздері мен бетті тани алмаған жағдайда, PIN кодтары мен үлгі кодтары әлі де осы құрылғыларда қосалқы бөлшектер ретінде қалды. Бұл технологияның қауіпсіздік және бақылау қосымшаларында кең таралуына әкелді.

Көздің сезімтал қабықшасының аутентификациясы. Көздің сезімтал қабықшасын сканерлеу аутентификацияның ең кең тараған биометриялық нысандарының бірі болып табылады (3-сурет).

Сурет 3. Көздің сезімтал қабықшасын тану

Адам көздеріндегі үлгілер бірегей және өмір бойы өзгермейді, бұл адамның шынайылығын тексеруге мүмкіндік береді. Тексеру үрдісі жеткілікті деңгейде күрделі, өйткені саусақ ізі сканерлерімен салыстырғанда көптеген нүктелер талданады, бұл жүйенің сенімділігін көрсетеді.

Көздің сезімтал қабықша үлгісінің күрделілігі өте жоғары сенімділік дәрежесін қамтамасыз етеді, сонымен қатар сканерлеу кезінде көзге түсетін әрі көзге көрінбейтін, жұмсақ жарықты пайдалануды қамтамасыз етеді. Бұл кейде жарқын жарықты пайдаланатын торды сканерлеуден ерекшеленеді.

Көз торының аутентификациясы. Тор қабықты сканерлеу – биометрияда адам көзін пайдаланудың балама жолы. Сканер көз алмасына жарқырап, қан тамырларының құрылымын көрсетеді, ол мембрана сияқты әрқайсымызға ғана тән.

Басқа биометриялық әдістерден айырмашылығы – торлы қабықты тану жоғары сапалы деректерді жинау үшін пайдаланушыдан көптеген көрсеткіштерді талап етеді. Пайдаланушы торды сканерлеу құрылғысына жақын болуы керек.

Тор қабық өте тұрақты болып саналады және адамның өмірі бойында іс жүзінде өзгеріссіз қалады. Осыған байланысты ол қазіргі нарықта бар ең сенімді биометриялық технология болып саналады.

Оқылатын және талданатын торлы қабықты тану деректерінің аз мөлшерін ескере отырып, жүйе адамның жеке басын тез растай алады. Торлы қабықтың көптеген ерекше белгілеріне байланысты жалған позитивтің ықтималдығы өте төмен.

Адам бетінің геометриясына негізделген аутентификация. Бет-әлпетті тану бірегей сандық үлгіні құру үшін бірге қолданылатын әртүрлі бет ерекшеліктерін пайдаланады. Мысалы, мұрынның пішіні немесе көздің арасындағы қашықтық қолданылады (4-сурет). Жалпы алғанда, бұл 80-нен астам түрлі белгілер.

Сурет 4. Адам бетінің геометриясын тану

Егер қолданба пайдаланушыны бет-жүзі бойынша анықтаса, сканерлеу сыймдылық камерасы арқылы жүзеге асырылады. Жоғары дәлдіктегі кескінді түсіру және пайдаланушының бет бейнесі бойынша 30 мыңнан астам бақылау нүктелерін тарату алгоритмі қажет [3].

Сканер геометриялық модель құру және оны сақтауға болатын есептеу нәтижелеріне айналдыру арқылы пайдаланушының бетін зерттейді деп айтуға болады. Авторизациялау кезінде белгілі бір пайдаланушыға арналған есептеу нәтижесі (қатені ескере отырып) жадта сақталған нәтижемен салыстырылады. Өндірушілер кәдімгі камераны пайдаланып 2D сканерлеумен шектелетін кездер болады. Әдетте, дерекқордағы басқа суреттермен салыстыруға болатын суретте бет ерекшеленеді.

Қолданба айырмашылықтарды таба алмаса, пайдаланушы иесі ретінде танылуы мүмкін. Бұл жағдайда әлеуетті шабуылдаушы иесінің фотосын сканерлеу арқылы қолданбаның құлпын ашу қаупі бар. Бұл мәселе тұлғаның егжей-тегжейлі құрылымдық картасын, сондай-ақ оның инфрақызыл спектрдегі бейнесін жасайтын заманауи инфрақызыл сканерлер арқылы шешіледі.

Мінез-құлық биометрикасы түрлері.

Дауысты тану. Дауысты тану ретінде адамның дауыстық сипаттамалары бойынша түпнұсқалығын растауды білдіреді. Түпнұсқалықты растау негізінен мәтінге тәуелді (пайдаланушы алдын ала анықталған сөзді немесе сөйлемді айтады) және аутентификация сіз сөйлейтін сөзге тәуелді болмаса да мәтінге тәуелсіз қол жеткізуге болады, дегенмен соңғысына жету қиынырақ міндет екені анық. Дауысты тану – бетті тану және пернелерді басу динамикасына ұқсас, ол құрылғыдағы бар аппараттық құралдарды пайдалана алады, дегенмен кейбір өндірушілер аутентификация алгоритмімен калибрленген белгілі бір микрофонды көрсетеді немесе қамтамасыз етеді.

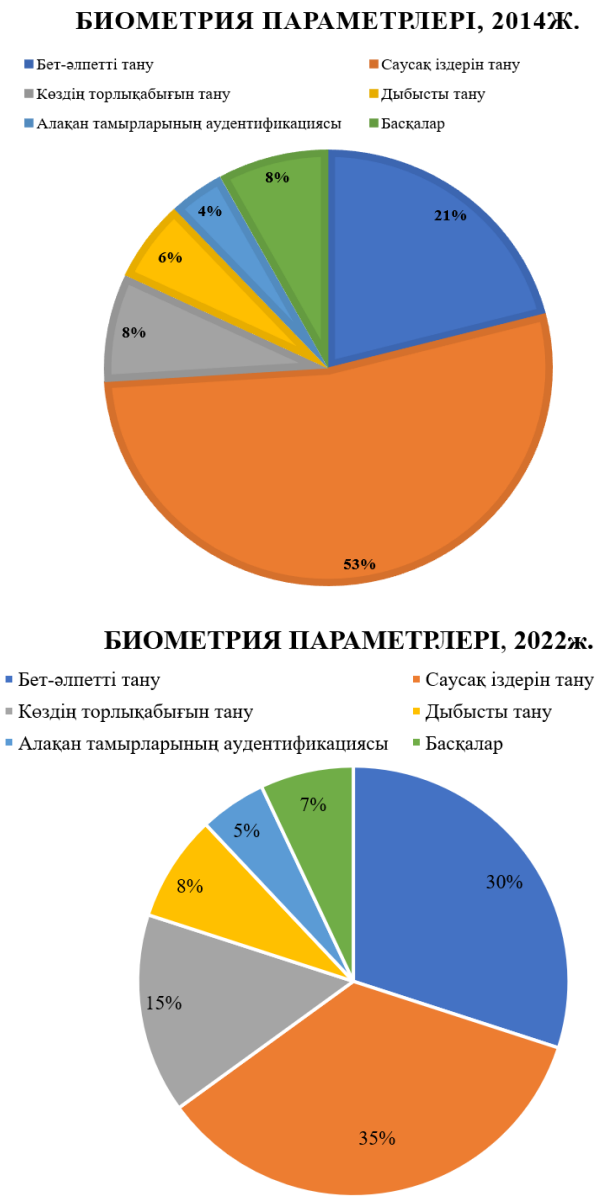
Қолтаңбаны тану. Бұл тәсілмен пайдаланушыларды аутентификациялау – адам қолтаңбасының ерекше аспектілерін пайдалану арқылы қол жеткізіледі. Қолтаңбаны танудың екі негізгі үрдісі бар: статикалық – мұнда толтырылған қолтаңба үлгі нұсқасымен салыстырылады және салыстыруға байланысты аутентификация беріледі; немесе динамикалық – мұнда жылдамдық, қысым және соққы реті сияқты мінез-құлық құрамдастары да ескеріледі, демек оның жалғандықты анықтау қабілеті жоғары. Сондықтан қолтаңбаны сканерлеу жүйелерінің көпшілігі жазу динамикасын тексере алатын электрондық планшетті пайдаланады.

Ғылыми нәтижелерді талқылау. Заманауи смартфондардағы биометрияның таралуын ескере отырып, қорғаныс деңгейін белгілі бір дәрежеде жақсартуға болатын бірнеше ұсыныстарды бөліп көрсете аламыз:

- экран бетінде қалған саусақ іздерінің көпшілігі бас бармақ пен сұқ саусақ іздері, сондықтан смартфонда аутентификация үшін басқа саусақтарды қолданған дұрыс;
- биометриялық тексерудің болуына қарамастан, күшті құпия сөзді немесе PIN-кодты пайдалану толық қауіпсіздіктің міндетті шарты болып табылады.

Аудентификациялаудың биометриялық әдістерін жалпы қолдану аймағы қарастыруда 2014 және 2022 жылғы жалпы дүниежүзі бойынша алынған сұрақтар бойынша қорытынды жасалған. Зерттеу нәтижесінде биометриялық параметрлер бойынша төмендегі көрсеткіштер алынған.

Биометриялық параметрлерге келесі көрсеткіштер жатады (5-сурет):



Сурет 5. Биометриялық параметрлер

2014 жылы саусақ іздері бойынша талдау 53% көрсетсе, ал 2022 жылы ол көрсеткіш 35% азайғандығын байқаймыз. Ал, бет-әлпетті тану көрсеткіші 2014 жылы 21% болса, 2022 жылы 30% көтерілгендігін көруге болады. Демек, саусақ іздерінен гөрі бет-әлпетті тану деңгейі едәуір артқан.

Қорытынды. Осылайша, биометриялық аутентификация тәсілдері өте ыңғайлы, себебі пайдаланушы код комбинациясын (құпия сөз) немесе үлгіні есте сақтаудың қажеті жоқ. Биометриканың айқын кемшілігі – осалдықтар көп, ал тану жүйесінің 100% сенімді болмауында.

Сонымен қатар, биометриялық параметрлерді (саусақ ізі немесе көздің сезімтал қабықша үлгісі) құпия сөз немесе PIN код сияқты өзгерту мүмкін емес. Бұл маңызды кемшілік, өйткені деректер бір рет шабуылдаушының қолына түссе, пайдаланушы өзін елеулі тәуекелдерге ұшыратады [4].

Саусақ ізін тану, бет-әлпетті тану және дауысты тану сияқты биометриялық қауіпсіздік шешімдері сәйкестендіру мен аутентификацияның жетілдірілген және сенімді әдістерін ұсынады. Бұл технологиялар кеңейтілген қауіпсіздік шараларын қамтамасыз етеді, олардың смартфондардан бастап қауіпсіздік деңгейі жоғары мекемелерге дейінгі қолданбалардың кең ауқымы үшін пайдасы зор. Биометриялық қауіпсіздік жүйелерін енгізу арқылы ұйымдар мен жеке тұлғалар құпия ақпараттың қорғалуын қамтамасыз етеді және жалпы қауіпсіздікті жақсарта алады.

Әдебиеттер тізімі

1. Технология биометрической аутентификации: как вас узнают машины? [Электронный ресурс]. – Режим доступа: https://copperpod.medium.com/the-technology-behind-biometric-authentication-how-do-machines-recognize-you-5f1f3fbc0ea3 Дата обращения 12.10.2023.
2. Биометрическая аутентификация: удобство или безопасность? [Электронный ресурс]. – Режим доступа: http://withsecurity.ru/biometricheskaya-autentifikaciya-preimushchestva-i-nedostatki .
3. Виды биометрии в мобильном приложении [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/simbirsoft/blog/529250/. Дата обращения 22.11.2020.
4. Биометрическая идентификация [Электронный ресурс]. – Режим доступа: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html Дата обращения 22.12.2020.

Материал редакцияға 13.03.24 түсті.

Ж.Е. Доумчариева[1], М.К. Есеналиева[1]

[1]Таразский региональный университет имени М.Х. Дулати, г. Тараз, Казахстан

БИОМЕТРИЧЕСКИЕ МЕТОДЫ АУТЕНТИФИКАЦИИ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Аннотация. В статье рассматривается понятие «биометрическая аутентификация», ее различные современные возможности, биометрические методы аутентификации, способы их использования, а также их преимущества и недостатки. Мобильные устройства заняли важное место в современном обществе: сегодня ими пользуются сотни миллионов человек. Надежная и нейтральная идентификация и аутентификация пользователей на мобильных устройствах, таких как смартфоны, сегодня является актуальным вопросом. Большинство современных решений в этой области основаны на сценарии «разблокировки устройства» – проверке информации (факторов аутентификации), предоставленной пользователем для разблокировки смартфона. Большинство из них используют слабые механизмы аутентификации, основанные на паролях и PIN-кодах, которые могут быть скомпрометированы, что позволяет злоумышленникам получить доступ к устройству и хранящимся на нем данным. Выявлена необходимость в строгой аутентификации, и обсуждается применение различных биометрических средств на мобильной платформе.

Ключевые слова: биометрическая аутентификация, отпечаток пальца, пользователь, сетевой источник, распознавание, сканирование.

Zh.E. Doumchariyeva[1], M.K. Yessenaliyeva[1]

[1]M.Kh Dulaty Taraz Regional University, Taraz, Kazakhstan

BIOMETRIC AUTHENTICATION METHODS ON MOBILE DEVICES

Abstract. The article discusses the concept of “Biometric Authentication”, various modern possibilities of biometric authentication, biometric authentication methods, methods of their use, as well as their advantages and disadvantages. Mobile devices have taken an important place in modern society: today they are used by hundreds of millions of people. Reliable and neutral identification and authentication of users on mobile devices such as smartphones are pressing issues today. Most modern solutions in this area are based on the “device unlocking” scenario - verifying information (authentication factors) provided by the user to unlock the smartphone. Most of them use weak authentication mechanisms based on passwords and PINs, which can be compromised, allowing attackers to gain access to the device and the data stored on it. The need for strong authentication is identified and the use of various biometrics on the mobile platform is discussed.

Keywords: biometric authentication, fingerprint, user, network source, recognition, scanning, Mobile Devices

References

1. Tekhnologiya biometricheskoy autentifikatsii: kak vas uznayut mashiny? [Biometric authentication technology: how do machines recognize you?] / [Electronic resource]. Access mode: https://copperpod.medium.com/the-technology-behind-biometric-authentication-how-do-machines-recognize-you-5f1f3fbc0ea3 (access date 12.10.2023) [in Russian].
2. Biometricheskaya autentifikatsiya: udobstvo ili bezopasnost'? [Biometric authentication: convenience or security?] / [Electronic resource]. Access mode: http://withsecurity.ru/biometricheskaya-autentifikaciya-preimushchestva-i-nedostatki [in Russian].
3. Vidy biometrii v mobil'nom prilozhenii [Types of biometrics in a mobile application] / [Electronic resource]. Access mode: https://habr.com/ru/company/simbirsoft/blog/529250/ (access date 22.11.2020) [in Russian].
4. Biometricheskaya identifikatsiya [Biometric identification] / [Electronic resource]. Access mode: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html (access date 22.12.2020) [in Russian].