

Е.Ә. Еркінбек

«Alikhan Bokeikhan University» ББМ

Семей қаласы, Қазақстан

e-mail: aliya_1991e@mail.ru

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТЕГІ БИОМЕТРИЯ. БИОМЕТРИЯЛЫҚ АУТЕНТИФИКАЦИЯНЫҢ БҮГІНІ ЖӘНЕ БОЛАШАҒЫ

Аннотация

Бұл мақалада қазіргі ақпараттық қоғам жағдайында адамның жеке басын растаудың маңызды аспектісі ретінде **биометриялық сәйкестендіру мен аутентификация** мәселесі қарастырылады. Дәстүрлі құпиясөздердің әлсіз жақтары мен қауіпсіздікке төнетін қатерлер талданады. Биометрияның негізгі түрлері — биологиялық, морфологиялық және мінез-құлықтық сипаттамалар — жан-жақты сипатталып, олардың артықшылықтары мен кемшіліктері көрсетіледі. Сонымен қатар, статикалық және динамикалық биометриялық аутентификация әдістері, олардың техникалық іске асу жолдары мен қауіпсіздік көрсеткіштері сараланады. Мақалада биометриялық жүйелердің сенімділігі, жалған оң және теріс нәтижелердің ықтималдығы, сондай-ақ жеке деректердің қауіпсіздігін қамтамасыз етуге қатысты тәуекелдер мен заманауи мәселелер қозғалады. Авторлар биометрияны қолданудың артықшылықтарымен қатар, оны ендірудегі техникалық және этикалық қиындықтарға да назар аударады.

Кілттік сөздер: Биометрия, аутентификация, сәйкестендіру, ақпараттық қауіпсіздік, саусақ ізі, бет пішінін тану, биометриялық деректер, авторизация, цифрлық қауіпсіздік, дербес деректерді қорғау.

Е.А. Еркінбек

УО «Alikhan Bokeikhan University»

г.Семей, Казахстан

e-mail: aliya_1991e@mail.ru

БИОМЕТРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. НАСТОЯЩЕЕ И ПЕРСПЕКТИВЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Аннотация

В этой статье рассматривается проблема биометрической идентификации и аутентификации как важнейшего аспекта подтверждения личности человека в условиях современного информационного общества. Анализируются слабые стороны традиционных паролей и угрозы безопасности. Основные виды биометрии: биологические, морфологические и поведенческие характеристики — всесторонне описаны и показаны их преимущества и недостатки. Кроме того, дифференцируются методы статической и динамической биометрической аутентификации, пути их технической реализации и показатели безопасности. В статье затрагиваются вопросы надежности биометрических систем, вероятности ложноположительных и отрицательных результатов, а также риски и современные проблемы, связанные с обеспечением безопасности персональных данных. Помимо преимуществ использования биометрии, авторы также обращают внимание на технические и этические проблемы, связанные с ее внедрением.

Ключевые слова: Биометрия, аутентификация, идентификация, информационная безопасность, отпечаток пальца, распознавание формы лица, биометрические данные, авторизация, цифровая безопасность, Защита персональных данных.

Y.A. Yerkinbek

"Alikhan Bokeikhan University"

Semey, Kazakhstan

e-mail: aliya_1991e@mail.ru

"Information Security in Biometrics: The Present and Future of Biometric Authentication"

Annotation

This article discusses the problem of biometric identification and authentication as the most important aspect of confirming a person's identity in the conditions of the modern Information Society. The weaknesses of traditional passwords and security threats are analyzed. The main types of biometrics — biological, morphological and behavioral characteristics—are described in detail and their advantages and disadvantages are indicated. In addition, static and dynamic biometric authentication methods, ways of their technical implementation and security indicators are differentiated. The article touches on the reliability of biometric systems, the likelihood of false positive and negative results, as well as risks and modern issues related to ensuring the security of personal data. In addition to the benefits of using biometrics, the authors also point to the technical and ethical challenges in its implementation.

Keywords: biometrics, authentication, identification, information security fingerprint, face shape recognition, biometric data, authorization, digital security, personal data protection

Кіріспе. Қазіргі заманда адамдар компьютерге, смартфонға және әртүрлі интернет-ресурстарға қол жеткізу үшін үнемі өз жеке басын растауға тура келеді. Пайдаланушылардың ыңғайлылығы үшін банкке бару, түрлі құжаттарды рәсімдеу және төлем жасау сияқты күнделікті істердің көпшілігі Интернетке көшірілді. Осыған байланысты жеке деректерді қорғау, сондай-ақ авторизацияланған қол жеткізуді қамтамасыз ету мәселесі өткір қойылып отыр.

Банкке келгенде адамдар өз жеке басын жеке куәлік арқылы растайды, бірақ интернет-банкинг жағдайында қалай болмақ? Көптеген жылдар бойы интернет-ресурстарға қол жеткізу үшін құпиясөздер пайдаланылды. Олардың идеологиясы мынада: құпиясөзді тек толық құқықты иелері ғана біледі. Өкінішке қарай, құпиясөздің анонимділігін жоғалту орасан зор салдарға әкелуі мүмкін, өйткені интернет-банктің құпиясөзі сейфтің кілтіне тең және ол қаскүнемге пайдаланушының қаржысына шексіз қол жеткізу мүмкіндігін береді. Осылайша, Интернеттегі идентификация және аутентификация мәселесі біздің заманымыздың басты проблемаларының біріне айналды.

Зерттеу әдістері:

1. Теориялық талдау әдісі. Биометрия, аутентификация, ақпараттық қауіпсіздік саласындағы отандық және шетелдік ғылыми әдебиеттерге, заңнамалық актілерге шолу жасалып, негізгі ұғымдар мен түсініктер талданды.

2. Жүйелік-құрылымдық әдіс. Биометриялық сәйкестендіру және аутентификация жүйелерінің құрылымы мен жұмыс істеу принциптері компоненттерге

бөлініп, олардың өзара байланысы мен логикалық құрылымы зерттелді.

3. Салыстырмалы талдау әдісі. Дәстүрлі (құпиясөз негізіндегі) және биометриялық аутентификация жүйелерінің артықшылықтары мен кемшіліктері салыстырылып, олардың сенімділігі мен қауіпсіздік деңгейі бағаланды.

4. Эмпирикалық (тәжірибелік) талдау элементтері. Қолданыстағы биометриялық жүйелердің (мысалы, саусақ ізі, бет-әлпет тану, тамыр үлгісі) жұмыс істеу алгоритмдері мен нақты қателік көрсеткіштері (FAR, FRR) негізінде техникалық тиімділікке баға берілді.

5. Қауіп-қатерлерді бағалау әдісі. Биометриялық деректердің бұзылу тәуекелі, заңсыз қол жеткізу ықтималдығы және этикалық мәселелер тұрғысынан қауіпсіздікке талдау жасалды.

Ақпараттық технологиялардың дамуымен жеке басын растаудың көптеген тәсілдері пайда бола бастады. Осы мақалада олардың ішіндегі ең қызықты әрі өзекті бағыттардың бірі — биометриялық идентификация мен аутентификацияға назар аударғым келеді.

Биометрия дегеніміз не?

Жалпы мағынасында биометрия — тірі ағзалардың дене сипаттамаларын өлшеуге және сипаттауға негізделген ғылым. Мысалы, саусақ іздерінің өрнегі, адамның бет пішіні немесе көздің тор қабығының суреті — биометриялық деректердің ең көп таралған түрлері, бірақ олармен шектелмейді.

Зерттеушілердің айтуынша, әрбір адамның денесінде көптеген бірегей параметрлер бар — адамның отыру немесе жүру мәнері, құлақ формасы, қолдағы тамырлардың орналасуы және тағы

басқалар. Дәл осы деректердің **қайталанбас ерекшелігі** биометриялық белгілерді жеке басын растау мәселесінде соншалықты танымал етті.

Биометриялық деректердің түрлері

Биометриялық деректерді шартты түрде үш топқа бөлуге болады:

1. Биологиялық биометрия
2. Морфологиялық биометрия
3. Мінез-құлық биометриясы

- Биологиялық биометрия – адамның генетикалық ерекшеліктеріне қатысты (ДНҚ, қан және т.б.). Оны сұйықтық үлгілері арқылы бағалауға болады.

- Морфологиялық биометрия – ең көп қолданылатын түрі, яғни адамның сыртқы ерекшеліктері: бет пішіні, саусақ ізі және т.б.

- Мінез-құлық биометриясы – адамның кейбір тұрақты мінез-құлық үлгілері: жүріс-тұрысы, сөйлеу мәнері немесе мимикасы.

Адамның генетикалық ерекшеліктеріне (ДНҚ, қан және т.б.) қатысты барлық нәрсе биологиялық биометрияға жатады. Оны сұйықтық үлгілерінің көмегімен бағалауға болады. Морфологиялық биометрия-қолданбалы қолдануда ең танымал, бұл адамның сыртқы ерекшеліктері: бет пішіні, саусақ ізі және т.б. мінез-құлық биометриясы адамның мінез-құлқында байқалатын кейбір үлгілерді білдіреді: жүру, сөйлеу мәнері немесе бет әлпеті.

Дәстүрлі Құпия сөздер әрқашан қауіпсіздік жүйелерінің әлсіз тұсы болды, өйткені оларды бұзу оңай. Биометрия, өз кезегінде, әлдеқайда күшті шешім болып табылады, сондықтан ол барған сайын танымал бола бастады. Қауіпсіздікті қамтамасыз ету үшін биометрияны қолданудың ең көп таралған мысалдары-бет пен дауысты тану және саусақ ізін сканерлеу.

Мақаланың басында біз биометрия сәйкестендіру және аутентификация үшін қолданылады деп айттық, бірақ бұл терминдердің айырмашылығы неде? Сәйкестендіру – бұл субъектіні оның идентификаторы арқылы тану процедурасы, ал аутентификация-аутентификация процедурасы. Егер біз бұл анықтамаларды Биометрия терминдеріне аударатын болсақ,

онда биометриялық сәйкестендіру-бұл жеке тұлғаны тану, яғни кез-келген ресурсқа қол жеткізуді қажет ететін барлық адамдардың таңдалған биометриялық белгілерінің үлгілерін сақтайтын мәліметтер базасы бар делік. Берілген белгіні дерекқорда сақталған барлық адамдармен салыстырған кезде, жүйе белгілі бір жүйеге жүгінетін адамның ондағы белгілері кім және кім екенін анықтайды. Биометриялық аутентификация-бұл өтініш берушінің жүйеге кіруге құқығы бар-жоғын анықтау үшін берілген белгіні дерекқорда сақталғанмен салыстыру процесі. Авторизация дегеніміз - белгілі бір адамға немесе адамдар тобына белгілі бір әрекеттерді орындау құқығын беру.

Биометриялық деректердің не екенін түсінгеннен кейін, оларды пайдалану ақпаратты рұқсатсыз кіруден қорғаудың жоғары сенімді әдісі деп болжауға болады. Бұл шынымен де солай, бірақ биометрияны аутентификация механизмі ретінде пайдалану кейбір асқынулар мен салдарға әкеледі.

Мұндағы бірінші мәселе-сканердің жалған теріс позитивтілігі. Мысалы, саусақ ізі арқылы пайдаланушының түпнұсқалығын тексеретін жүйе саусақтың кесілуіне, сканерге кірдің түсуіне немесе шамадан тыс ылғалға байланысты кіруден бас тартуы мүмкін. Биометрика жүйеде бірнеше авторизация нұсқаларының бірі болып табылатын жағдайларда, мысалы, смартфондарда саусақ ізін дұрыс оқымаған кезде пайдаланушыдан құпия сөзді енгізу сұралады, бұл мәселе емес. Биометриялық мәліметтер жеке тұлғаны растаудың жалғыз әдісі болып табылатын жүйелерде бұл толыққанды пайдаланушының жеке басын тексере алмауына әкеледі.

Екінші мәселе – технологияның дамуы туралы заңға бағынатын азаматтар ғана емес, зиянкестер де біледі. Бірнеше жылдан бері, мысалы, бейнежазбада бір адамның бетін екіншісіне ауыстыруға мүмкіндік беретін технологиялар бар, бұл хакерлерге бет сканерін алдауға мүмкіндік береді. Сканерге адамның динамикалық бейнеклонын беру үшін ықтимал жәбірленушінің фотосуреті болуы жеткілікті. Егер саусақ ізін сканерлеу туралы айтатын болсақ, онда бәрі де тегіс емес:

оларды латекс пішінімен, қолғаппен немесе тіпті жоғары ажыратымдылықтағы алақанның фотосуретімен қолдан жасауға болады. Бұл мәселені биометриялық аутентификацияның барлық жаңа әдістері мен түрлерін әзірлеу арқылы шешуге тырысады.

Ең маңызды мәселе-биометриялық деректердің бұзылуы. Егер шабуылдаушылар парольді ұрласа, оны бірнеше минут ішінде өзгертуге болады. Ұрланған несие картасын немесе таңбалауышты қалпына келтіру ұзағырақ уақыт алады, бірақ иесі үшін әлі де үлкен мәселе болмайды. Бірақ егер адам оның биометриясын ұрласа не болады? Біз биометрика туғаннан бастап адамға тиесілі және олар ерекше екендігі туралы айттық. Сондықтан мұндай деректерді ұрлау кезінде жеке басын ұрлау орын алады. Адам ешқайда қоңырау шалып, өзіне жаңа бетке немесе саусақ ізіне тапсырыс бере алмайды, өйткені шабуылдаушылар олардың толық көшірмелеріне қандай да бір жолмен қол жеткізді. Бұл биометрияны қолданудың үлкен қаупі. Қазіргі уақытта биометриялық аутентификация әдістерінің екі класы бар: статикалық әдістерге негізделген және динамикалық әдістерге негізделген.

Биометриялық аутентификацияның статикалық әдістері

Статикалық әдістер адамның туылғаннан бастап болатын биометриялық сипаттамаларына негізделген.

Бет геометриясының аутентификациясы ең күрделі техникалық іске асырумен сипатталады. Әдіс адам бетінің үш өлшемді моделін құруға негізделген, ол үшін әртүрлі элементтердің контурлары және пайдаланушының бетінің сипаттамалық нүктелері ерекшеленеді, олардың арасындағы қашықтық есептеледі. Бірегей үлгіні анықтау үшін 12-ден 40-қа дейін тән элементтер қажет. Бірегей үлгі кескіннің көптеген вариацияларын ескеруі керек. Бұл объектіге (бетке) тор проекцияланады. Әрі қарай, камера секундына ондаған кадр жылдамдығымен суретке түсіреді және алынған суреттер арнайы бағдарламамен өңделеді. Қисық бетке түскен сәуле бүгіледі-бетінің қисықтығы неғұрлым үлкен болса, сәуленің

иілісі соғұрлым күшті болады. Бастапқыда "жалюзи" арқылы берілетін көрінетін жарық көзі қолданылды. Содан кейін көрінетін жарық инфрақызылға ауыстырылды, ол аз жарық жағдайында немесе тіпті толық қараңғыда жұмыс істей алады. Алынған суреттерге сәйкес, қажетсіз кедергілер (шаш, сақал, мұрт және көзілдірік) ерекшеленетін және жойылатын беттің 3D моделі қалпына келтіріледі. Содан кейін модельге талдау жасалады – антропометриялық ерекшеліктер ерекшеленеді, нәтижесінде олар мәліметтер базасына енгізілген бірегей кодқа жазылады. Суретті түсіру және өңдеу уақыты ең жақсы модельдер үшін 1-2 секундты құрайды.

Frr (false Rejection Rate, бірінші қателік) және far (false Acceptance Rate, екінші қателік) туралы толық деректер өндірушілердің сайттарында осы сыныптың алгоритмдері үшін ашық түрде берілмеген. Бірақ bioscript фирмасының ең жақсы модельдері үшін (3D EnrolCam, 3D FastPass) (суретті қараңыз. 1) Үлгіні проекциялау әдісі бойынша жұмыс істейтін far = 0,0047% frr 0,103% құрайды. Айта кету керек, бірінші және екінші типтегі қателіктердің шамалары бір-бірімен байланысты және олардың біреуін төмендету әрекеттері сөзсіз екіншісінің өсуіне әкеледі. Ақ саласында екінші типтегі қате (заңсыз пайдаланушының ресурсына рұқсат беру) ең маңызды болып саналады, сондықтан олар бірінші типтегі қатеге (заңды пайдаланушының ресурсына жол бермеу) ақылға қонымды шектеулер қою арқылы оны азайтуға тырысады. Сипатталған әдістің статистикалық сенімділігі саусақ ізін аутентификациялау әдісімен салыстыруға болады деп саналады.

Әдістің артықшылығы ретінде сканерлеу құрылғысымен байланысқа түсудің қажеті жоқ және адамның өзінде (көзілдіріктің пайда болуы, сақал, шаштың өзгеруі) және оның айналасында (жарықтандыру, бастың айналуы) сыртқы факторларға төмен сезімталдықты атап өтуге болады. Саусақ ізінің аутентификация метімен салыстыруға болатын сенімділіктің жоғары деңгейі де байқалады.

Әдістің негізгі кемшілігі-жабдықтың жоғары құны. Сатылымда бар кешендер тіпті ирис сканерлерінен де жоғары. Сонымен қатар, бет әлпетінің өзгеруі және бет әлпеті әдістің

статистикалық сенімділігін нашарлатады. Әдіс әлі де жақсы дамымаған, әсіресе ұзақ уақыт бойы қолданылған саусақ ізімен салыстырғанда, оны кеңінен қолдануды қиындатады.

Тамыр үлгісі бойынша Аутентификация. Әдістің негізі-алақанның сыртын немесе ішкі жағын суретке түсіретін инфракызыл (ИК) камера. Қанның гемоглобині ИҚ сәулесін сіңіретіндіктен тамырлардың үлгісі қалыптасады. Нәтижесінде шағылысу дәрежесі төмендейді және тамырлар камерада қара сызықтар түрінде көрінеді. Алынған мәліметтер негізінде арнайы бағдарлама сандық конволюцияны жасайды. Frr және FAR мәні Palm vein сканері үшін берілген (суретті қараңыз. 2). Әзірлеушінің мәліметтері бойынша, far-да 0,0008% FRR

дәлдік көрсеткіштерін айтарлықтай нашарлатады. Бұл әдіс биометрияның басқа статикалық әдістерімен салыстырғанда әлі аз зерттелген.

Бас сүйегінің құрылымы бойынша аутентификация. Штутгарт университетінің зерттеушілер тобы он түрлі адамның бас сүйектері арқылы бірдей дыбыс толқындарын өткізіп, қызықты эксперимент жүргізді. Алынған нәтижелер SkullConduct құрылғысын құруға негіз болды. Белгілі болғандай, барлық адамдардың бас сүйектері әртүрлі, сондықтан олар арқылы өтетін дыбыс толқындары әртүрлі сипаттамаларға ие, оларды кейінірек сәйкестендіру мен аутентификацияның жаңа түрі ретінде пайдалануға болады. Оның тиімділігі 97% жетеді. Екі өткізгіш тақтайшадан тұратын



0,01% құрайды. Дәлірек деректерді бірде-бір өндіруші ашпайды.

Сурет 2. Palm сканері бар құрылғылардың мысалы Vein.

Әдістің негізгі артықшылықтары-сканерлеу құрылғысымен байланысқа түсудің қажеті жоқ және жоғары сенімділік: әдістің статистикалық көрсеткіштерін ирис көрсеткіштерімен салыстыруға болады. Сипаттаманың жасырындығын атап өткен жөн. Жоғарыда келтірілген биометрияның барлық мысалдарынан айырмашылығы, бұл сипаттаманы қылмыстық мақсатта "көшеде" адамнан алу өте қиын, мысалы, оны камерамен суретке түсіру.

Әдістің кемшіліктері сканердің сезімталдығымен және адамның тамырларындағы мүмкін өзгерістермен байланысты. Сканерді күн сәулесімен және галоген шамдарының сәулелерімен жарықтандыруға жол берілмейді. Кейбір жасқа байланысты аурулар, мысалы, артрит

skullconduct гарнитурасы бет сүйектерінің жоғарғы жағына құлақтың жанына бекітіледі. Қазіргі уақытта SkullConduct сынақтан өтуде: зерттеушілер оның тиімділігін арттыру үшін жұмыс істеуде.

Әдістің негізгі артықшылықтары-сипаттаманың жасырылуы және жүйені тозуға болатын электроникаға біріктіру мүмкіндігі (суретті қараңыз. 3). Негізгі кемшіліктер-адаммен байланыс және пайдалану кезінде пайда болатын шу.



Сурет 3. Интеграция SkullConduct Google Glass-да.

Биометриялық аутентификацияның динамикалық әдістері

Статикалық әдістерде қолданылатын биометриялық сипаттамалардың өзгермейтіндігі мен ашықтығы биометриялық кілтті қолдан жасауға мүмкіндік береді. Нәтижесінде биометриялық аутентификацияның динамикалық әдістерін қолданудың бірқатар артықшылықтары бар.

Жүрек сипаттамалары бойынша Аутентификация. 2017 жылдың қыркүйегінде биометриялық аутентификацияның жаңа әдісі – жүрек арқылы белгілі болды. Мұндай даму Буффало университетінде ойлап табылды. Оның мәні әр 8 секунд сайын адамның жүрегінің пішінін, өлшемін және ЭКГ-ны анықтауға мүмкіндік беретін төмен деңгейлі Доплер радиолокаторын пайдалану болып табылады. Егер осы уақыт ішінде жүйеге жүктелген пайдаланушының жүрегі анықталмаса, компьютер бұғатталады.

Жоба авторлары сканер адам ағзасына зиянсыз деп санайды, өйткені оның сәулеленуі тек 5 мВт құрайды, бұл қазіргі заманғы смартфондардың сәулеленуінің 1% - дан азына сәйкес келеді. Сонымен қатар, құрылғының прототипінде смартфонның өзі жүрек белсенділігі сканері ретінде әрекет етеді (суретті қараңыз. 4).



Сурет 4. Смартфонды сканер ретінде пайдалану.

Бұл әдістің артықшылығы-сканерлеу құрылғысымен байланысу қажеттілігінің болмауы ғана емес, сонымен қатар 30 м-ге дейінгі қашықтықта жұмыс істеу мүмкіндігі. Бұл оны адамдар көп жиналатын жерлерде жеке тұлғаны қатесіз тексерудің ықтимал сұранысқа ие және ыңғайлы тәсілі етеді. Сонымен қатар, жүйе төмен қуат тұтынумен сипатталады, бұл оны тек стационарлық компьютерлерде ғана емес, мобильді құрылғыларда да тиімді пайдалануға мүмкіндік береді. Негізгі кемшілік-кейбір ауруларда жүрек жұмысының формасы мен ритмінің өзгеру мүмкіндігі.

Болашақта пайдаланушының жүрек-қантамыр жүйесінің параметрлері мен олардың комбинацияларын қолданатын авторизациялық әдістердің әртүрлі вариациялары пайда болады: жүректің микровибрациясы, жүрек ритмі және т. б.

Ерін қозғалысының аутентификациясы. Ерін аутентификациясы технологиясы 2015 жылы Гонконг баптисттік университетінде әзірленді және патенттелді. Оның негізі текстураны және мимиканы ескере отырып, мысалы, парольді айту кезінде еріннің тән қимылдарын тану болып табылады. Ғалымдардың пікірінше, мұндай биометриялық след қолдан жасау мүмкін емес.

Ерінді сәйкестендіру қауіпсіздік жүйелерінің тиімділігін арттыру үшін қолданылуы мүмкін және бетті тану, көз

торын сканерлеу, саусақ ізі сияқты қол жеткізу әдістеріне қосымша ретінде қызмет етеді. Технологияны пилоттық қолдануды банкоматтарда қызмет көрсету және қоғамдық орындарға кіруді бақылау үшін енгізу жоспарлануда.

Технологияның артықшылығы-бұрыннан бар бет сканеріне қосымша ретінде әрекет ету мүмкіндігі, оның көшірмесін жасау міндетін едәуір қиындатады. Кемшілігі-нақты бейнені жасау үшін әртүрлі эмоцияларды ұзақ сканерлеу қажеттілігі.

Саусақ микро дірілінің аутентификациясы. Нью-Брансуиктегі Ратгерс университетінің инженерлері 2017 жылдың күзінде адамдарды авторизациялаудың тағы бір қызықты динамикалық әдісін ұсынды – саусақ микровибрациясы. Зерттеушілер әр қолданушы үшін олар ерекше болады және сәйкесінше жеке қолтаңба пайда болуы мүмкін, оны жалған жасау өте қиын болады.

Vibwrite деп аталатын жүйе өте қарапайым жұмыс істейді: қатты бетке-ағаш, металл, пластик немесе әйнек болсын – арзан діріл қозғалтқышы мен сенсор бекітіледі; адам саусағымен бетіне тигенде, қозғалтқыштың діріліне бірегей қолтаңба ретінде оқылатын кедергілер енгізіледі (суретті қараңыз. 5).

Сонымен қатар, олар әр саусақ үшін ерекше болады және олардың қысқа мерзімділігі авторизацияның сенімділігін арттырады, әсіресе кодты енгізумен, графикалық кілттермен, сондай-ақ технологияны жасаушылар дәстүрлі биометриялық құралдармен сендіреді.



Сурет 5. Орнату VibWrite.

Биометриялық әдістерге негізделген авторизация жүйелерінің таралуымен оларды айналып өту жолдарының саны да

артып келеді. Зерттелген технологиялардың ішіндегі ең перспективалысы-қолданыстағы кешендерді дәйекті немесе параллельді пайдалану мүмкіндігімен толықтыратындар. Сонымен, бетті танудың заманауи жүйелерінің қауіпсіздігін мимика мен жылу карталарын есепке алу мүмкіндігімен жақсартуға болады. Саусақ іздері жүйелері саусақ микровибрациясы мен сүйек өткізгіштігін оқи алады. Осылайша, биометриялық өнімділікті қолдан жасау міндеті жүйенің жұмыс жылдамдығы мен ыңғайлылығын жоғалтпай өте күрделі болады.

Зерттеу нәтижелері

Зерттеу барысында биометриялық аутентификацияның теориялық және практикалық аспектілері жан-жақты талданды. Сәйкестендіру мен аутентификация процестерінің мәні мен айырмашылықтары нақтыланып, биометрияның қауіпсіздік жүйелеріндегі артықшылықтары мен тәуекелдері анықталды.

Қорытынды

Қорытындылай келе, биометриялық аутентификация өте сенімді және ыңғайлы деп айтуға болады. Кез-келген кілтті немесе картаны алып жүрудің қажеті жоқ, әсіресе әр түрлі парольдерді басыңызда ұстаудың қажеті жоқ – бәрі әрқашан өзіңізбен бірге болады. Бірақ мұндай технологияларды қолдана отырып, сіз әрқашан тәуекелдер мен салдарлар туралы ойлануыңыз керек, өйткені абсолютті қорғаныс жоқ және кез-келген жүйе осал.

Пайдаланылған әдебиеттер тізімі:

1. Баймульдин М.К. Ақпараттық жүйелердің қауіпсіздігі. Оқу құралы.- Алматы., 2019
2. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры. Учебник.- М, 2020.
3. Актаева, А.У. Ақпараттық қауіпсіздік және қорғау: техникалық құрылғылар. 2-бөлім: Оқулық.- Алматы, 2019.
4. Маляревский, Ю.Д. Биометрические технологии идентификации личности. – М. : Радио и связь, 2007. – 240 с.
5. Мальцев, С.В. Информационная безопасность. Биометрические системы аутентификации. – СПб. : Питер, 2019. – 192 с. – (Серия: Учебное пособие).
6. Голованов, Н.А., Шевченко, И.Н. Современные биометрические технологии идентификации личности // Информационные технологии и вычислительные системы. – 2020. – №3. – С. 45–52.
7. Шустов, Л.Н. Биометрия в системах информационной безопасности // *Вестник ВГУ. Серия: Системный анализ и информационные технологии*. – 2018. – №2. – С. 112–118.
8. Омарова С.А. Основы информационных систем и информационная безопасность. Учебное пособие.- Алматы, 2023
9. Jain, A.K., Ross, A., Prabhakar, S.
An Introduction to Biometric Recognition // *IEEE Transactions on Circuits and Systems for Video Technology*. – 2004. – Vol. 14, No. 1. – P. 4–20.
10. Ключев, Е.В. Безопасность информационных систем. – М. : Горячая линия – Телеком, 2016. – 288 с.

Pajdalangan adebietter tizimi

1. Bajmul'din M.K. Aқпараттық жүйелердің қауіпсіздігі. Оқу құралы.- Алматы., 2019
2. Il'in, M.E. Kriptograficheskaya zashchita informacii v ob'ektah informacionnoj infrastruktury. Uchebnik.- M, 2020.
3. Aktaeva, A.U. Aқпараттық қауіпсіздік және қорғау: tekhnikalық құрылғылар. 2-bөлім: Оқулық.- Almaty, 2019.
4. Malyarevskij, YU.D. Biometricheskie tekhnologii identifikacii lichnosti. – M. : Radio i svyaz', 2007. – 240 s.
5. Mal'cev, S.V. Informacionnaya bezopasnost'. Biometricheskie sistemy autentifikacii. – SPb. : Piter, 2019. – 192 s. – (Seriya: Uchebnoe posobie).
6. Golovanov, N.A., Shevchenko, I.N. Sovremennye biometricheskie tekhnologii identifikacii lichnosti // Informacionnye tekhnologii i vychislitel'nye sistemy. – 2020. – №3. – S. 45–52.
7. SHustov, L.N. Biometriya v sistemah informacionnoj bezopasnosti // *Vestnik VGU. Seriya: Sistemnyj analiz i informacionnye tekhnologii*. – 2018. – №2. – S. 112–118.
8. Omarova S.A. Osnovy informacionnyh sistem i informacionnaya bezopasnost'. Uchebnoe posobie.- Almaty, 2023
9. Jain, A.K., Ross, A., Prabhakar, S.
An Introduction to Biometric Recognition // *IEEE Transactions on Circuits and Systems for Video Technology*. – 2004. – Vol. 14, No. 1. – P. 4–20.
10. Klyuev, E.V. Bezopasnost' informacionnyh sistem. – M. : Goryachaya liniya – Telekom, 2016. – 288 s.

Автор жайлы мәлімет:

Еркінбек Әлия Еркінбекқызы

Лауазымы: «Alikhan Bokeikhan University» ББМ , Ақпараттық-техникалық ғылымдары
кафедрасының аға оқытушысы, магистр

Ұялы телефон: +77071243591

E-mail: aliya_1991e@mail.ru

Сведения об авторе:

Еркинбек Алия Еркинбеккызы

Должность: УО «Alikhan Bokeikhan University», старший преподаватель кафедры
Информационно-технических наук, магистр

Мобильный телефон: +77071243591

E-mail: aliya_1991e@mail.ru

Information about the author:

Yerkinbek Aliya Yerkinbekkyzy

Position: Senior Lecturer of the Department of Information and technical sciences of the
educational institution" Alikhan Bokeikhan University", Master

Mobile phone: +77071243591

E-mail: aliya_1991e@mail.ru