AUTENTIFIKATSIYA MUAMMOLARI, USULLARI VA VOSITALARI

Fozilov Shavkatjon Ibrohimjon o'g'li,
NamDU o'qituvchisi
Tel: +998939623333
E-mail: shavkatmanager@gmail.com
Yo'ldosheva Maftuna Zokirjon qizi,
NamDU Magistranti

ANNOTATSIYA

Ushbu maqola autentifikatsiya tizimlarida eng katta muammo sifatida foydalanuvchining autentigikatsiya vositasiga begona shaxslarning egalik qilishi ko'rsatilgan. Shu muammoni bartaraf etish uchun biometrik vositalar keltirilgan.

Kalit so'zlar: *autentifikatsiya, biometrik, barmoq izi, parol, avtorizatsiya.*

ПРОБЛЕМЫ, МЕТОДЫ И СРЕДСТВА АУТЕНТИФИКАЦИИ

Фозилов Шавкатжон Ибрагимжон угли,
НамГУ. Учитель
Тел: +998939623333
E-mail: shavkatmanager@gmail.com
Юлдашева Мафтуна Зокиржон кизи,
НамГУ. Мастер

АННОТАЦИЯ

В этой статье указывается, что самая большая проблема с системами аутентификации заключается в том, что третьи стороны владеют инструментом аутентификации пользователей. Для решения этой проблемы предусмотрены биометрические инструменты.

Ключевые слова: *аутентификация, биометрия, отпечаток пальца, пароль, авторизация.*

PROBLEMS, METHODS AND TOOLS OF AUTENTIFICATION

Fozilov Shavkatjon Ibrahimjon ugli,
NamSU. Teacher
Tel: +998939623333
Email: shavkatmanager@gmail.com
Yuldasheva Maftuna Zokirjon kizi,
NamSU. Master

ABSTRACT

This article points out that the biggest problem with authentication systems is that third parties own the user authentication tool. Biometric tools are provided to overcome this problem.

Keywords: *authentication, biometrics, fingerprint, password, authorization.*

KIRISH

Autentifikatsiya (Authentication) – ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatan aynan o'zi ekanligiga ishonch xosil qilishiga imkon beradi. Autentifikatsiya o'tqazishda tekshiruvchi taraf tekshiriluvchi tarafning xaqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qatnashadi.Odatda foydalanuvchi tizimga o'z xususidagi noyob, boshqalarga ma'lum bo'lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Autentifikatsiya natijasida foydalanuvchilarni shaxsini aniqlash(tekshirish) va unga tarmoq xizmatlaridan foydalanishga ruxsat berish vazifalari amalga oshiriladi.O'zining haqiqiyligining tasdiqlash uchun sub'ekt tizimga turli asoslarni ko'rsatishi mumkin. Sub'ekt ko'rsatadigan asoslarga bog'liq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga bo'linishi mumkin:

- biror narsani bilish asosida. Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda "so'rov javob" xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko'rsatish mumkin;
- biror narsaga egaligi asosida. Odatda bular magnit kartalar, smartkartalar, sertifikatlar va "touch memory" qurilmalari;
- qandaydir daxlsiz xarakteristikalar asosida. Ushbu kategoriya o'z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko'zining rangdor pardasi va to'r pardasi, barmoq izlari, kaft geometriyasi va x.) asoslangan usullarni oladi. Biometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

MUHOKAMA VA NATIJALAR

Biometrik autentifikatsiyalash jaroyonida foydalanuvchining shaxsan biologik belgilari olinadi va bu belgilar boshqalarda uchramaydi, shuning uchun ham bu usul boshqa autentifikatsiya usullaridan ishonchli hisoblanadi. Undantashqari foydalanuvchining bu shaxsiy belgilari ko'chirib foydalanib bo'lmaydi, ya'ni uning

aynan ishtirokida amalga oshiriladi. Bundan kelib chiqib biometric belgilarni ikkita katta guruhga ajratish mumkin:

1. Fizikbelgilar(barmoqizlari, ko'zto'rpardasi, yuzshakli);
2. Psixiologikbelgilar(klaviaturaorqaliimzochekish, ovozorqali).

Bu ikki turdan fizik belgilar orqali autentifikatsiyalsh ishonchli hisoblanadi, chunki psixik belgilar vaziyatga qarab har xil bo'lishi mumkin.

Autentifikatsiya tizimlarida eng katta muammo foydalanuvchining autentigikatsiya vositasiga begona shaxslarning egalik qilishi. Ushbu kamchilikni bartaraf etish uchun bevosita beometrik vositalarga tayanamiz. Chunki ularning aynan shaxsning o'zisiz foydalanish mumkin emas.

Ushbu biometrik parametrlarni ochiq tarmoqda uzatish xavfli, shuning uchun uni xavfsiz kanallardan uzatish muammosi xam tug'iladi.

Foydalanuvchilarni identifikatsiya va autentifikatsiyadan o'tkazish asosan tizimdan foydalanishga ruxsat berish uchun amalga oshiriladi. Ma'lumotlarni uzatish kanallarida himoyalashda sub'ektlarning o'zaro autentifikatsiyasi, ya'ni aloqa kanallari orqali bog'lanadigan sub'ektlar xaqiqiyligining o'zaro tasdig'I bajarilishi shart. Xaqiqiylikning tasdig'i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. "Ulanish" atamasi orqali tarmoqning ikkita sub'ekti o'rtasida mantiqiy bog'lanish tushuniladi. Ushbu muolajaning maqsadi – ulanish qonuniy sub'ekt bilan amalga oshirilganligiga va barcha axborot mo'ljallangan manzilga borishligiga ishonchni ta'minlashdir.

Elektron tijorat tizimida to'lovlar quyidagi qator shartlarning bajarilishi asosida amalga oshiriladi:

- konfidentsiallikning saqlanishi – Internet orqali to'lovlar amalga oshirilishida xaridor ma'lumotlarining (masalan, kredit karta nomeri) faqat qonun bilan belgilangan tashkilotlargina bilishi kafolatlanishi shart;
- axborot yaxlitligining saqlanishi-xarid xususidagi axborot hech kim tomonidan o'zgartirilishi mumkin emas;
- autentifikatsiya-xaridorlar va sotuvchilar ikkala tomon ham haqiqiy ekanligiga ishonch hosil qilishlari shart;
- to'lov vositalarining qulayligi - xaridorlarga qulay bo'lgan har qanday vositalar bilan to'lov imkoniyati;
- avtorizatsiya - jarayoni, bu jarayon kechuvida tranzaktsiya o'tkazilishi xususidagi talab to'lov tizimi tomonidan ma'qullanadi yoki rad etiladi. Bu muolaja xaridorning mablag'i borligini aniqlashga imkon beradi;

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o'ziga xos masalalarni yechishga imkon beradi.Shu sababli autentifikatsiya jarayonlari va protokollari amalda faol ishlatiladi. Shu bilan bir qatorda ta'kidlash lozimki, nullik bilim bilan isbotlash xususiyatiga ega bo'lgan autentifikatsiyaga qiziqish amaliy xarakterga nisbatan ko'proq nazariy xarakterga ega.Balkim, yaqin kelajakda ulardan axborot almashinuvini himoyalashda faol foydalanishlari mumkin.

Autentifikatsiya protokollariga bo'ladigan asosiy xujumlar quyidagilar:

•maskarad (impersonation). Foydalanuvchi o'zini boshqa shaxs deb ko'rsatishga urinib, u shaxs tarafidan xarakatlarning imkoniyatlariga va imtiyozlariga ega bo'lishni mo'ljallaydi;

- autentifikatsiya almashinuvi tarafini almashtirib qo'yish (interleaving attack). Niyati buzuq odam ushbu xujum mobaynida ikki taraf orasidagi autenfikatsion almashinish jarayonida trafikni modifikatsiyalash niyatida qatnashadi. Almashtirib qo'yishning quyidagi xili mavjud: ikkita foydalanuvchi o'rtasidagi autentifikatsiya muvaffaqiyatli o'tib, ulanish o'rnatilganidan so'ng buzg'unchi foydalanuvchilardan birini chiqarib tashlab, uning nomidan ishni davom ettiradi;
- takroriy uzatish (replay attack). Foydalanuvchilarning biri tomonidan autentifikatsiya ma'lumotlari takroran uzatiladi;
- uzatishni qaytarish (reflection attak). Oldingi xujum variantlaridan biri bo'lib, xujum mobaynida niyati buzuq odam protokolning ushbu sessiya doirasida ushlab qolingan axborotni orqaga qaytaradi.
- majburiy kechikish (forsed delay). Niyati buzuq odam qandaydir ma'lumotni ushlab qolib, biror vaqtdan so'ng uzatadi.
- matn tanlashli xujum (chosen text attack). Niyati buzuq odam autentifikatsiya trafigini ushlab qolib, uzoq muddatli kriptografik kalitlar xususidagi axborotni olishga urinadi.

Yuqorida keltirilgan xujumlarni bartaraf qilish uchun autentifikatsiya protokollarini qurishda quyidagi usullardan foydalaniladi:

– "so'rov–javob", vaqt belgilari, tasodifiy sonlar, indentifikatorlar, raqamli imzolar kabi mexanizmlardan foydalanish;

– autentifikatsiya natijasini foydalanuvchilarning tizim doirasidagi keyingi xarakatlariga bog'lash. Bunday misol yondashishga tariqasida autentifikatsiya jarayonida foydalanuvchilarning keyinga o'zaro aloqalarida ishlatiluvchi maxfiy seans kalitlarini almashishni ko'rsatish mumkin;

– aloqaning o'rnatilgan seansi doirasida autentifikatsiya muolajasini vaqti-vaqti bilan bajarib turish va h.

Autentifikatsiya protokollarini taqqoslashda va tanlashda quyidagi xarakteristikalarni hisobga olish zarur:

– o`zaro autentifikatsiyaning mavjudligi. Ushbu xususiyat autentifikatsion almashinuv taraflari o`rtasida ikkiyoqlama autentifikatsiyaning zarurligini aks ettiradi;

– hisoblash samaradorligi. Protokolni bajarishda zarur bo`lgan amallar soni;

– kommunikatsion samaradorlik. Ushbu xususiyat autentifikatsiyani bajarish uchun zarur bo`lgan xabar soni va uzunligini aks ettiradi;

– uchinchi tarafning mavjudligi. Uchinchi tarafga misol tariqasida simmetrik kalitlarni taqsimlovchi ishonchli serverni yoki ochiq kalitlarni taqsimlash uchun sertifikatlar daraxtini amalga oshiruvchi serverni ko`rsatish mumkin;

– xavfsizlik kafolati asosi. Misol sifatida nullik bilim bilan isbotlash xususiyatiga ega bo`lgan protokollarni ko`rsatish mumkin;

– sirni saqlash. Jiddiy kalitli axborotni saqlash usuli ko`zda tutiladi.

Autentifikatsiya jarayoni quyidagi xizmatlar uchun qo’llaniladi:

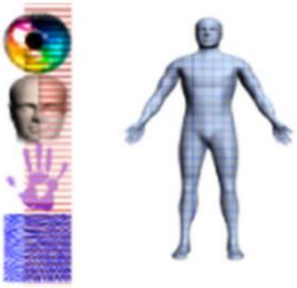
- Elektron pochta;
- Web forum;
- Umumiy tarmoqda;
- Internet-bank tizimida;
- To’lov tizimlarida;
- Korparativ tarmoqlarda;
- Internet magazinda;

Tarmoqda qo’llaniladigan xizmatlar va qurilmalarning muhimligiga ko’ra autentifikatsiyaning turli usullaridan foydalaniladi(1-rasm).

Autentifikatsiyani tanitishning asosan ikki xil yo’nalish mavjud:

- Onlayn tanish usullari
- Offlayn tanish usullari

Bu autentifikatsiyalash jarayonida foydalanuvchi ma’lumotlarining belgilarini o’zgarishi sistemaga kirishni murakkablashtiradi va “HA” yoki “YO’Q” javobi orqali tizimga kirishi mumkin. Biometrik belgilarning o’zgarishi ham “YO’Q” javobini berishga sabab bo’lishi mumkin.

Axborot tashuvchilar	ID-karta USB-kalit ID-manzil	
Axborot	Parol PIN-kod Ixtiyoriy so'z	
Biometrik	Barmoq izi Yuz geometriyasi Bioimzo Ko'z to'rpardasi Ovoz, qon tomir	

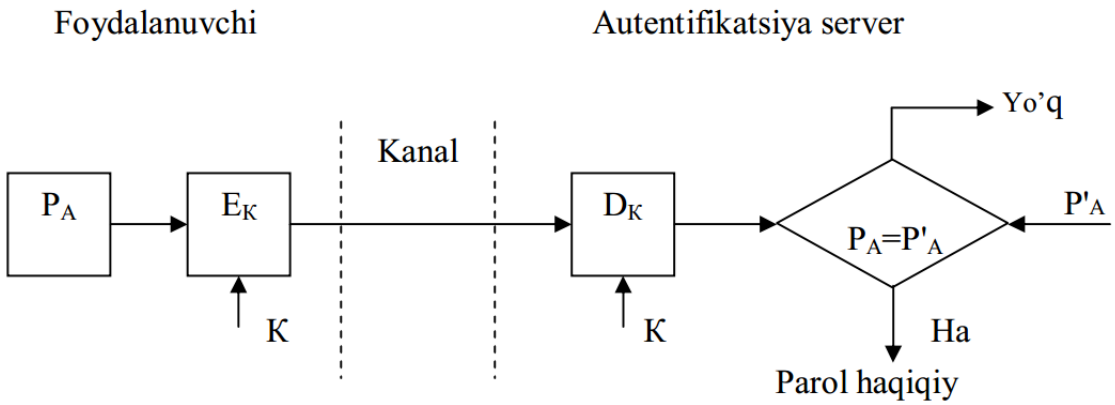
1-rasm. Autentifikatsiya usullari

Parollar asosida autentifikatsiyalash. Autentifikatsiyaning keng tarqalgan sxemalaridan biri oddiy autentifikatsiyalash bo'lib, u an'anaviy ko'p martali parollarni ishlatishiga asoslangan.Tarmoqdagi foydalanuvchini oddiy autentifikatsiyalash muolajasini quyidagicha tasavvur etish mumkin. Tarmoqdan foydalanishga uringan foydalanuvchi kompyuter klaviaturasida o'zining identifikatori va parolini teradi. Bu ma'lumotlar autentifikatsiya serveriga ishlanish uchun tushadi. Autentifikatsiya serverida saqlanayotgan foydalanuvchi identifikatori bo'yicha ma'lumotlar bazasidan mos yozuv topiladi, undan parolni topib foydalanuvchi kiritgan parol bilan taqqoslanadi. Agar ular mos kelsa, autentifikatsiya muvaffaqiyatli o'tgan hisoblanadi va foydalanuvchi legal (qonuniy) maqomini va avtorizatsiya tizimi orqali uning maqomi uchun aniqlangan xuquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi.

Paroldan foydalangan holda oddiy autentifikatsiyalash sxemasi 2–rasmda keltirilgan.

Foydalanuvchining parolini shifrlamasdan uzatish orqali autentifikatsiyalash varianti xavfsizlikning xatto minimal darajasini kafolatlamaydi. Parolni himoyalash uchun uni himoyalanmagan kanal orqali uzatishdan oldin shifrlash zarur. Buning uchun sxemaga shifrlash E_K va rasshifrovka qilish D_K vositalari kiritilgan. Bu vositalar bo'linuvchi maxfiy kalit K orqali boshqariladi. Foydalanuvchining haqiqiyligini tekshirish foydalanuvchi yuborgan parol P_A bilan autentifikatsiya

serverida saqlanuvchi dastlabki qiymatni taqqoslashga asoslangan. Agar P_A va qiymatlar mos kelsa, parol P_A haqiqiy, foydalanuvchi A esa qonuniy hisoblanadi.



2-rasm. Paroldan foydalangan holda oddiy autentifikatsiyalash

Sertifikatlar asosida autentifikatsiyalash. Tarmoqdan foydalanuvchilar soni millionlab o'lchanganida foydalanuvchilar parollarining tayinlanishi va saqlanishi bilan bog'liq foydalanuvchilarni dastlabki ro'yxatga olish muolajasi juda katta va amalga oshirilishi qiyin bo'ladi. Bunday sharoitda raqamli sertifikatlar asosidagi autentifikatsiyalash parollar qo'llanishiga ratsional alternativ hisoblanadi.

Raqamli sertifikatlar ishlatilganida kompyuter tarmog'i foydalanuvchilari xususidagi hech qanday axborotni saqlamaydi. Bunday axborotni foydalanuvchilarning o'zi so'rov-sertifikatlarida taqdim etadilar. Bunda maxfiy axborotni, xususan maxfiy kalitlarni saqlash vazifasi foydalanuvchilarning o'ziga yuklanadi.

Foydalanuvchi shaxsini tasdiqlovchi raqamli sertifikatlar foydalanuvchilar so'rovi bo'yicha maxsus vakolatli tashkilot-sertifikatsiya markazi CA (Certificate Authority) tomonidan, ma'lum shartlar bajarilganida beriladi.Ta'kidlash lozimki, sertifikat olish muolajasining o'zi ham foydalanuvchining haqiqiyligini tekshirish (ya'ni, autentifikatsiyalash) bosqichini o'z ichiga oladi.Bunda tekshiruvchi taraf sertifikatsiyalovchi tashkilot (sertifikatsiya markazi CA) bo'ladi.

Sertifikat olish uchun mijoz sertifikatsiya markaziga shaxsini tasdiqlovchi ma'lumotni va ochiq kalitini taqdim etishi lozim. Zaruriy ma'lumotlar ro'yxati olinadigan sertifikat turiga bog'liq. Sertifikatsiyalovchi tashkilot foydalanuvchining haqiqiyligi tasdig'ini tekshirganidan so'ng o'zining raqamli imzosini ochiq kalit va foydalanuvchi xususidagi ma'lumot bo'lgan faylga joylashtiradi hamda ushbu ochiq kalitning muayyan shaxsga tegishli ekanligini tasdiqlagan holda foydalanuvchiga sertifikat beradi.

Sertifikat elektron shakl bo'lib, tarkibida qo'yidagi axborot bo'ladi:

- ushbu sertifikat egasining ochiq kaliti;
- sertifikat egasi xususidagi ma'lumot, masalan, ismi, elektron pochta manzili, ishlaydigan tashkilot nomi va h.;
- ushbu sertifikatni bergan tashkilot nomi;
- sertifikatsiyalovchi tashkilotning elektron imzosi – ushbu tashkilotning maxfiy kaliti yordamida shifrlangan sertifikatsiyadagi ma'lumotlar.

Qat'iy autentifikatsiyalash. Kriptografik protokollarida amalga oshiriluvchi qat'iy autentifikatsiyalash g'oyasi quyidagicha.Tekshiriluvchi (isbotlovchi) taraf qandaydir sirni bilishini namoyish etgan holda tekshiruvchiga o'zining haqiqiy ekanligini isbotlaydi. Masalan, bu sir autentifikatsion almashish taraflari o'rtasida oldindan xavfsiz usul bilan taqsimlangan bo'lishi mumkin. Sirni bilishlik isboti kriptografik usul va vositalardan foydalanilgan holda so'rov va javob ketma-ketligi yordamida amalga oshiriladi. Eng muhimi, isbotlovchi taraf faqat sirni bilishligini namoyish etadi, sirni o'zi esa autentifikatsion almashish mobaynida ochilmaydi.Bu tekshiruvchi tarafning turli so'rovlariga isbotlovchi tarafning javoblari yordami bilan ta'minlanadi. Bunda yakuniy so'rov faqat foydalanuvchi siriga va protokol boshlanishida ixtiyoriy tanlangan katta sondan iborat boshlang'ich so'rovga bog'liq bo'ladi. Aksariyat hollarda qat'iy autentifikatsiyalashga binoan har bir foydalanuvchi o'zining maxfiy kalitiga egalik alomati bo'yicha autentifikatsiyalanadi. Boshqacha aytganda foydalanuvchi uning aloqa bo'yicha sherigining tegishli maxfiy kalitga egaligini va u bu kalitni axborot almashinuvi bo'yicha haqiqiy sherik ekanligini isbotlashga ishlata olishi mumkinligini aniqlash imkoniyatiga ega.

X.509 standarti tavsiyalariga binoan qat'iy autentifikatsiyalashning quyidagi muolajalari farqlanadi:

- bir tomonlama autentifikatsiya;
- ikki tomonlama autentifikatsiya;
- uch tomonlama autentifikatsiya.

Bir tomonlama autentifikatsiyalash bir tomonga yo'naltirilgan axborot almashinuvini ko'zda tutadi. Autentifikatsiyaning bu turi quyidagilarga imkon yaratadi:

- axborot almashinuvchining faqat bir tarafini haqiqiyligini tasdiqlash;
- uzatilayotgan axborot yaxlitligining buzilishini aniqlash;
- "uzatishning takrori" tipidagi xujumni aniqlash;
- uzatilayotgan autentifikatsion ma'lumotlardan faqat tekshiruvchi taraf foydalanishini kafolatlash.

Ikki tomonlama autentifikatsilashda bir tomonliligiga nisbatan isbotlovchi tarafga tekshiruvchi tarafning qo'shimcha javobi bo'ladi.Bu javob tekshiruvchi tomonni aloqaning aynan autentifikatsiya ma'lumotlari mo'ljallangan taraf bilan o'rnatilayotganiga ishontirish lozim.

Uch tomonlama autentifikatsiyalash tarkibida isbotlovchi tarafdan tekshiruvchi tarafga qo'shimcha ma'lumotlar uzatish mavjud.Bunday yonda-shish autentifikatsiya o'tkazishda vaqt belgilaridan foydalanishdan voz kechishga imkon beradi.

USB kalitlar va Smart kartalar. Hozirda parollar asosida autentifikatsiyalash keng tarqalgan ya'ni 60% foydalanuvchilar foydalanadi. Lekin uning xavfsizlikni ta'minlash imkoniyati unchalik ham ta'minlanmagan, shuning uchun hozirgi kunda USB kalitlar va smart kartalarasosida autentifikatsiyalash keng tarqalmoqda.

USB kalitlarni bir ko'rinishi sifatida E-Tokenni keltirsak bo'ladi. U apparatura va dasturlar orqali amalga oshirilib autentifikatsiyalovchi tizimda ya'ni, USB qurilmada elektron raqamli imzo saqlanadi. Uning ko'rinishi quyidagicha bo'lishi mumkin: eToken PRO - USB-kalit(3-rasm).

3-rasm. USB va Smart kartalar

Ular bir martalik va ko'p martalik kalit generatsiya qilinishi bilan farqlanadi. Masalan: Aladdin firmasi tomonidan tayyorlangan 32k va 64k versiyali USB qurilmalari bir martalik kalit asosida ishlaydi ya'ni har bir foydalanishda yangi kalit hosil qilib turadi. Uni amalga oshirish uchun dastur yoki apparatura va eToken NG-OTP - gibrid USB-kalit kerak bo'ladi . Hozirda Alladin firmasi tomonidan ishlab chiqilgan smart kartalar xuddi eTokenlar bajargan ishlarni xam amalga oshiradi.

Lekin muammoni bir tarafi hal bo'lgani bilan ikkinchi tarafi shundaki, smart kartalarni ishlatish uchun kompyuterda yana boshqa qurilma zarur lekin eToken uchun shart emas. Bundan tashqari eTokenlar faqat kalitlarni emas ixtiyoriy maxfiy ma'lumotlar, sertifikatlar va boshqa ma'lumotlarni xavfsiz saqlashi mumkin. Agar

eTokenda tizimga kiruvchi PIN(Personal Identification Number) saqalngan bo'lsa, u %systemroot%\system32\etcpass.ini faylidagi ma'lumotni o'zgartirib qo'yadi. Va tizimga kirishda faqat shu eToken ichidagi parol orqali kiriladi. Foydalanuvchini autentifikatsiyalashda faol ishlatiladigan biometrik usullar quyidagilar:

- barmoq izlari;
- qo'l panjasining geometrik shakli;
- yuzning shakli va o'lchamlari;
- ovoz xususiyatlari;
- ko'z yoyi va to'r pardasining naqshi;
- elektron imzo orqali.

Biometrik autentifikatsiyalash usullari an'anaviy usullarga nisbatan quyidagi afzalliklarga ega:

- biometrik alomatlarning noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqori;
- biometrik alomatlarning sog'lom shaxsdan ajratib bo'lmasligi;
- biometrik alomatlarni soxtalashtirishning qiyinligi.

XULOSA

Biometrik autentifikatsiyada foydalanuvchini tasdiqlovchi shaxsiy ma'lumotlar xavfsiz kanallar orqali uzatilishi lozim. Chunki kanalda uzatilayotgan ma'lumotlarni(login, parol) ushlab qolish xavflarini kamaytirish lozim. Buning maxsus vositachi dasurlardan, kriptografik algoritmlardan va virtual kanallardan foydalanish lozim.

REFERENCES

1. Fozilov, S. I. O. G. L. (2022). OVOZNI TANISH ALGORITMLARI. *Oriental renaissance: Innovative, educational, natural and social sciences*, *2*(5-2), 553-562.
2. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems, " IBM systems Journal, vol. 40, p. 614-634.
3. Magnuson, S (January 2009), "Defense department under pressure to share biometric data.", NationalDefenseMagazine.org.
4. M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition, " presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.