AVTOMATLASHTIRILGAN TIZIMLARDA FOYDALANUVCHI PAROLINI TANLASH STRATEGIYASI HAMDA HIMOYA QILISH USULLARI

Zaripov Nozimbek Nayimovich
Buxoro davlat pedagogika instituti Aniq fanlar kafedrasi dotsenti, p.f.f.d (PhD).

Hasanov Behzod Normurot o'g'li
Buxoro davlat pedagogika instituti Matematika va informatik yo'nalishi 2-bosqich talabasi

Protasov Yorqinjon Yoqubjon o'g'li
Buxoro davlat pedagogika instituti Matematika va informatika yo'nalishi 1-bosqich talabasi

Annotatsiya. *Mazkur maqolada foydalanuvchilar avtomatlashtirilgan elektron tizimlarda parol tanlashda kamdan-kam holatlarda \ topilishi qiyin va oson esda qoladigan parol tanlashlari, bu esa tizim xavfsizligini susaytirashi va muammoni yechishda, foydalanuvchilar parol qo'yish siyosati talablarini bilishlari kerakligi bayon etilgan.*

Kalit so'zlar: *foydalanuvchi, parol, shifrlash, xavfsizlik, globallashuv, axborot, avtomatlashtirilgan tizimlar.*

Аннотация. *В данной статье указано, что при выборе паролей в автоматизированных электронных системах пользователи редко выбирают пароли, которые трудно подобрать и легко запомнить, что ослабляет безопасность системы, и при решении проблемы пользователям следует знать о требованиях политики паролей.*

Ключевые слова: *пользователь, пароль, криптография, безопасность, глобализация, информации, автоматизированные системы.*

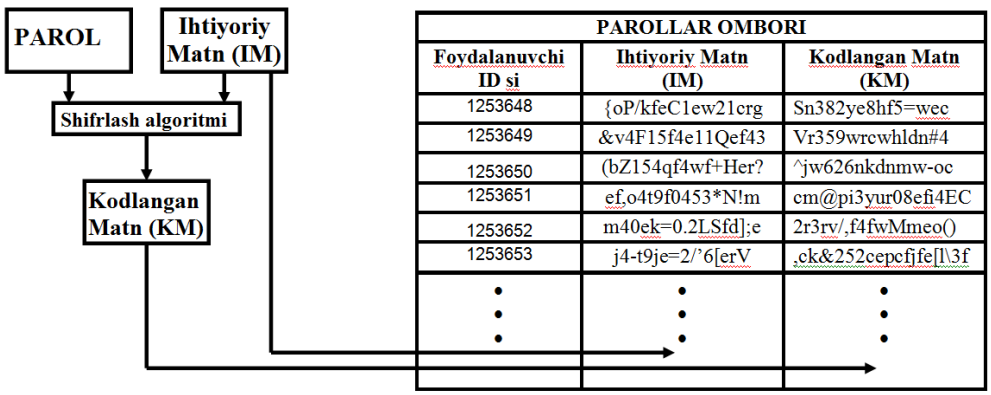
Abstract*. This article states that when choosing passwords in automated electronic systems, users rarely choose passwords that are hard to find and easy to remember, which weakens the system's security, and when solving the problem, users should be aware of password policy requirements.*

Key words: *user, password, cryptography, security, globalization, information, automated system.*

Bugungi globallashuv jarayonida insonlarga qulaylik yaratish maqsadida juda ko‘p avtomatlashtirilgan elektron tizimlar tatbiq qilinmoqda. Bunday tizimlarga bank, soliq, hukumat tizimi, tashkilot va ta’lim tizimlari kabi juda ko‘p misollar olishi mumkin. Tizimga kirish uchun foydalanuvchilar o‘zlarining login (tizimdagi ism) va paroliga ega bo‘lishi zarur. Ularning login va parollari tizim ma’lumotlari omborida maxsus unikal kod-identifikator (ID) bilan farqlanadi. Foyadalanuvchi paroli tizim himoyasining old qatori hisoblanadi. Parol tizim ma’lumotlar omboridagi foydalanuvchi IDsini aniqlaydi. Identifikatorga foydalanuvchi haqida quyidagi ma’lumotlar beriladi:

- ID foydalanuvchi ro‘yxatdan o‘tgan-o‘tmaganligini va qancha vaqt foydalanish huquqi berilganligini aniqlaydi;
- ID foydalanuvchiga qanday rol berilganligini aniqlaydi, ya’ni foydalanuvchi faqat ma’lumotdan foydalanishi yoki qo‘shimcha uni tahrirlashi mumkin;
- ID foydalanuvchining to‘liq ma’lumotlarini aniqlaydi.

Foydalanuvchi paroli tizim uchun muhim ahamiyatga egaligini anglash maqsadida elektron tizimlarda foydalanuvchi parolini himoya qilishning eng samarali usullaridan biri – parolni yashirish, uni ochiq holda qoldirmaslikni quyidagi sxemada ko‘ramiz.



1-rasm. Foydalanuvchi parolini kiritish yoki yangilash jarayoni

Ushbu 1-rasmda keltirilgan sxemada foydalanuvchi tomonidan kiritiladigan parol faqat tizimga ma’lum bo‘lgan ixtiyoriy o‘zgaradigan matn (IM) bilan shifrlash qoidalari asosida kodlanadi va hosil bo‘lgan kodlangan matn (KM) foydalanuvchi paroli sifatida ma’lumotlar omboriga joylashtiriladi. Parollar omborida

foydalanuvchining asl paroli o'rniga boshqa kodlangan matn hosil bo'lishi tizimning xafsizligini kuchaytiradi. Bu foydalanuvchi parolisiz tizimga kirish imkoni yoqligini yoki bu uchun ko'p vaqt ketishini anglatadi.

Kodlangan matnni topish murrakabligini oshirish maqsadida tizimning IM ga quyidagicha talablar qo'yiladi:

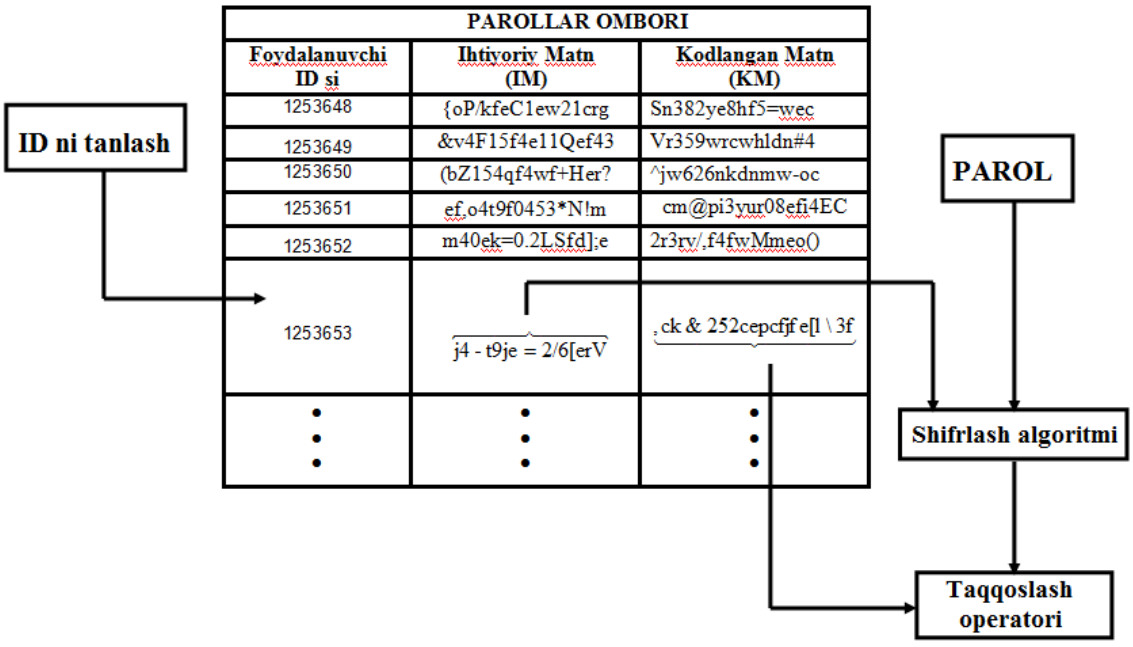
•Bir-xil parollar bo'lishini oldini oladi, ya'ni bir nechta foydalanuvchilar bir-xil parol qoyganda ham IM orqali turli-xil kodga o'zgaradi;

•Parol uzunligini ortiradi va bu parolni topilish ehtimolini pasaytiradi. Agar IM ning uzunligi 16 ga teng bo'lsa, KM ning uzunligi o'z-o'zidan 16 dan katta bo'ladi;

•Foydalanuvchilar porol qo'yishidagi kamchiliklarini tuzatadi.

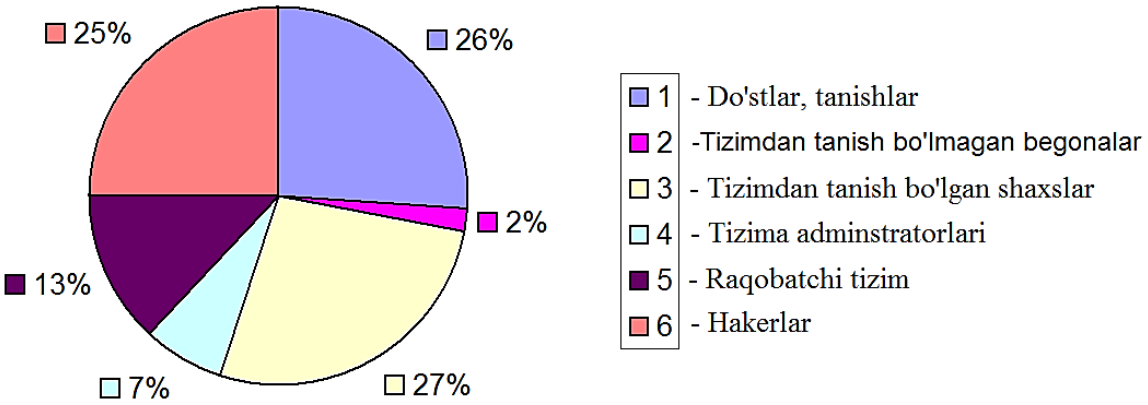
Foydalanuvchi tizimga qayta kirishida, foydalanuvchi paroli dastlab parollar omboridagi IM bilan shifrlash algoritimida kodlanadi va ombordagi KM bilan taqqoslanadi. Shundan so'ng foydalanuvchiga tizimga kirishga ruxsat beriladi (2-rasm) .

Tizim xavfsizligi mutaxassis dasturchilar, tizim adminstratorlari tomonidan mustahkamlangandan so'ng muammo foydalanuvchi parolida qoladi. Agar foydalanuvchi o'z parolini birovga oshkor qilsa yoki topilishi oson bo'lgan parol qoysa, tizimga ruxsatsiz kiruvchilar hosil bo'ladi. Buning natijasida ma'lumotlar omborining yaxlitligi buziladi va tizimning xafsizligi buziladi.



2-rasm: Foydalanuvchi parolini tasdiqlash

Tizimda ruxsatsiz, foydalanuvchilar parolini bilgan holda kimlar kirishi mumkinligi haqida quyidagi statistik ma’lumot keltiramiz (3-rasm):



3-rasm. Foydalanuvchi paroli orqali tizimga ruxsatsiz kiruvchilar

Albatta, harf, raqam va maxsus belgilardan mukammal tuzilgan sakkiz belgili parol doimiy xafsizlik garovi bo‘la olmaydi. Kompyuter texnalogiyalaring tez rivojlanib borishi, ularning ishlash tezligi oshgan holda millionlab vazifalarni bir soniyada bajarishi ehtimoldan xoli emas. Ammo bu ma’lum bir vaqt talab etadi. Shuning uchun parolni tez-tez yangilab turish maqsadga muvofiq.

Misol sifatida elektron bank tizimini olaylik. Juda ko‘p rivojlangan davlatlar bank tizimlarida, mijozlar e-banking xizmatidan foydalanish va o‘zlarining hisob sahifalariga ko‘rish uchun quyidagilarni kiritishadi:

•Login – o‘zgarmas, bankda dastlabki ro‘yxatdan o‘tishda beriladi;

•Parol – foydalanuvchi tomonidan ixtiyoriy vaqtda o‘zgartirish mumkin;

•Kalit – bu bank tomonidan berilgan elektron qurilmadan kiritiluvchi sonlar;

Kalit elektron qurilmasidagi sonlar qisqa vaqt ichida (20-30 soniyada) ixtiyoriy o‘zgaradi, bu o‘zgarish bankning ro‘yxatdan o‘tqazuvchi serveridagi sonlar bilan bir-xil vaqtda va bir-xil sonlarga o‘zgaradi. (4-rasm).

4-rasm. Elektron raqamli kalit

Avtomatlashtirilgan elektron tizimlarning ortib borishi foydalanuvchilarga ularga kirish parolini eslab qolish yoki havfsiz parol qo'yish muammosini olib kelmoqda.

Parol(ing. password) bu - amaliy munosabat boshlash uchun ishlatiladigan, subyektning siri hisoblanadigan identifikator. Tizimga kirish uchun klaviatura tugmalarini bosish ketma-ketligi. Parol simvollar (harflar, raqamlar, maxsus belgilar) kombinatsiyasi bo'lib, uni faqat parol egasi bilishi kerak.

Axborot xavfsizligini ta'minlash uchun foydalanuvchilarni **identifikatsiyalash, autentifikatsiyalash, avtorizatsiyalash** zarur bo'ladi.

Identifikatsiya – foydalanuvchini tizimga o'zini tanitish jarayoni bo'lib, unda mijozning maxsus shaxsiy kartalaridan yoki uning biometrik xususiyatlaridan foydalaniladi. Axborot xavfsizligini ta'minlash uchun shaxsning, masalan, **barmoq izi, ovoz tahlili, ko'z qorachig'i, yuz tuzilishi** va boshqa **biometrik** belgilaridan foydalaniladi.

Autentifikatsiya – foydalanuvchining to'g'riligi tekshiriladi va uning asosida tizimda faoliyat olib borishi mumkinligi yoki mumkin emasligi belgilanadi.

Avtorizatsiya — foydalanuvchiga tizim tomonidan berilgan huquqlar majmuasidir.

Ma'lumotni ochish – tasodifan yoki xusumatli harakatlar natijasida begona shaxsga axborotning mazmuni ruxsatsiz oshkor etishdir.

Axborotni muhofazalash – bu ma'lumotlarni o'g'irlash, yo'qotish, soxtalashtirish, qalbakilashtirsh, ruxsatsiz foydalanish va ko'paytirishning oldini olishga yo'naltirilgan tadbirlar majmuasidir.

Axborot xavfsizligi – foydalanish talablari asosida ma'lumotning yashirinligi, yaxlitligi va foydalanuvchanligini ta'minlashdir.

Kompyuterning zamonaviy operatsion tizimlarida paroldan foydalanish o'rnatilgan. Parol xeshlangan holatda kompyuterning qattiq diskida saqlanadi. Parollarni taqqoslash operatsion tizim (OT) tomonidan foydalanuvchi huquqiga mos imkoniyatlar yuklangunga qadar amalga oshiriladi. Lekin, kompyuterning OTdan foydalanishda kiritiladigan foydalanuvchi parolidan tashqari, Internetda ro'yxati keltirilgan ayrim «texnologik» parollardan ham foydalanish mumkin. Ko'pgina kompyuter tizimlarida identifikator sifatida, foydalanishga ruxsat

etilgan subyektni identifikatsiyalovchi kod yozilgan yechib olinuvchi axborot tashuvchilardan foydalaniladi.

Foydalanuvchilarni identifykatsiyalashda, tasodifiy identifikatsiyalash kodlarini hosil qiluvchi – elektron jetonlardan keng foydalaniladi. Jeton – bu, harflar va raqamlarning tasodifiy ketma-ketligini (so‘zni) yaratuvchi qurilma. Bu so‘z kompyuter tizimidagi xuddi shunday so‘z bilan taxminan minutiga bir marta sinxron tarzda o‘zgartirib turiladi. Natijada, faqatgina ma’lum vaqt oralig‘ida va tizimga faqatgina bir marta kirish uchun foydalanishga yaraydigan, bir martalik parol ishlab chiqariladi. Boshqa bir turdagi jeton tashqi ko‘rinishiga ko‘ra kalkulyatorga o‘xshab ketadi. Autentifikatsiyalash jarayonida kompyuter tizimi foydalanuvchi monitoriga raqamli ketma-ketlikdan iborat so‘rov chiqaradi, foydalanuvchi ushbu so‘rovni jeton tugmalari orqali kiritadi. Bunda jeton o‘z indikatorida akslanadigan javob ketma-ketligini ishlab chiqadi va foydalanuvchi ushbu ketma-ketlikni kompyuter tizimiga kiritadi. Natijada, yana bir bor bir martalik qaytarilmaydigan parol olinadi. Jetonsiz tizimga kirishning imkoni bo‘lmaydi. Jetondan foylanishdan avval unga foydalanuvchi o‘zining shaxsiy parolini kiritishi lozim.

Atrubutivli identifikatorlardan (parollardan tashqari) ruxsat berilish va qayd qilish chog‘ida foydalanilish mumkin yoki ular ish vaqti tugagunga qadar ishlatilayotgan qurilmaga doimiy ulangan holda bo‘lishi shart. Qisqa vaqtga biror joyga chiqilganda ham identifikator olib qo‘yiladi va qurilmadan foydalanish blokirovka qilinadi. Bunday apparat-dasturiy vositalar nafaqat qurilmalardan foydalanishni cheklash masalalarini hal qila oladi, shu bilan birga axborotlardan noqonuniy foydalanishdan himoyalashni ta’minlaydi. Bunday qurilmalarning ishlash prinsipi qurilmaga o‘rnatilgan OT funksiyalarini kengaytirishga asoslangan.

Autentifikatsiyalash jarayoni kompyuter tizimlari bilan ruxsat etilgan subyekt orasida amalga oshiriladigan dialogni ham o‘z ichiga olishi mumkin. Ruxsat etilgan subyektga bir qator savollar beriladi, olingan javoblar tahlil qilinadi va ruxsat etilgan subyektning aslligi bo‘yicha yakuniy xulosa qilinadi.

Kompyuter tizimlarining xotira qurilmalarida, odatda tizim konfiguratsiyasi haqidagi ma’lumotlar saqlanadi. Bunday ma’lumotlarga: qurilmaning (bloklarning)

turi va ularning tavsiflari, tashqi qurilmalarning soni va ulanish sabablarini o'ziga xos xususiyatlari, ish rejimlari va boshqalarni kiritish mumkin. Konfigursiyaning muayyan tuzilishi kompyuter tizimlarining va OTning turiga qarab aniqlanadi. Har qanday holatda ham dasturiy vositalar yordamida KT konfiguratsiyasi haqidagi ma'lumotlarni yig'ish va taqqoslashni tashkil etish mumkin. Agar kompyuter tarmoqda ishlayotgan bo'lsa, hech bo'lmaganda uni tarmoqqa ulash paytida kompyuterning konfiguratsiyasi nazoratdan o'tkaziladi. Nazoratning yanada ishonchli va tezkor usuli, qurilmaning maxsus kod – identifikatoridan foydalanish hisoblanadi. Bu kod qurilma vositalarida hosil qilinadi va xotira qurilmasida saqlanishi mumkin.

Himoyalovchi apparat-dasturiy komplekslarning ko'pchiligi maksimal sondagi himoyalash mexanizmlaridan foydalaniladi. Bu mexanizmlarga quyidagilar kiritish mumkin:

–foydalanuvchilarni identifykatsiyalash va autentifikatsiyalash;

– fayllar, papkalar, disklardan foydalanishga ruxsatni cheklash;

– dasturiy vositalar va axborotlar butunligini nazorat qilish;

– foydalanuvchi uchun funksional yopiq muhitni yaratish imkoniyati;

– OTni yuklanish jarayonini himoyalash;

– foydalanuvchi yo'qligida kompyuterni blokirovka qilish;

– ma'lumotlarni kriptografik o'zgartirish;

– hodisalarni qayd qilish;

– xotirani tozalash.

Axborotni muhofaza qilishda yetarli darajadagi yutuqlarga erishish uchun huquqiy, tashkiliy va texnik choralarni birgalikda amalga oshirish zarur. Bu himoyalanadigan axborotning konfedensialligi, tahdidning tasnifi va himoya vositalarining mavjudligi bilan belgilanadi. Umumiy holda xavfsizlikni ta'minlashning kompleks choralariga quyidagilarni kiritish mumkin:

– ruxsatsiz foydalanishdan kompleks himoya qilish vositalari;

– apparat-dasturiy vositalar;

– kriptografik muhofaza qilishning kompleks vositalari;

– injener-texnik tadbirlar;

– texnik kanallarni blokirovkalash kompleks vositalari;

Bu choralarning har biri boshqasini to'ldiradi, bironta usulning yo'qligi yoki yetishmasligi yetarli darajadagi himoyaning buzilishiga sabab bo'lishi mumkin.

Hozirgi kunda elektron tizimlarga kirish uchun

foydalanuvchi tomonidan qo‘llanadigan parol tez-tez yangilanib turilishi va belgilar soni sakkiztadan ko‘p bo‘lgan raqamlar, katta-kichik harflar va !@#$%^&*()_+”?>+=< kabi belgilar birlashmasidan iborat bo‘lishi maqsadga muvofiqdir.

Foydalanilgan adabiyotlar:

1. Henk C.A.. van Tilborg, Sushil Jajodia. Encyclopedia of Cryptography and Security. -NY.: Springer, 2011.-P. 957-958.

2. William Stallings. Cryptography and Network Security Principles and Practices., Fifth Edition. -NY.: Pearson, 2011.-P. 769-775.

3. Zaripov N.N.. «Kompyuter grafikasi» O‘quv qo‘llanma – Buxoro, “Durdona”, 2020. - 202 b.

4. Zaripov N.N.. «Delphi dasturlash muhitida komponentalar bilan ishlash texnologiyalari». O‘quv qo‘llanma. – Buxoro, “ Durdona” nashriyoti,2020. - 128 b.

5. G‘aniyev S.K., M.M. Karimov, K.A. Toshev. Axborot xafsizligi. Axborot-kommunikatsiya tizimlari xafsizligi. T.: “Aloqachi”, 2008, - 379 b.

6. Shirley Gaw, Edward W. Felten. Password Management Strategies for Online Accounts. Princeton University, 2002, -P. 25-27.

7. Carol Tice, Neil Tortorella “Freelance Business Bootcamp How to Launch, Earn, and Grow into a Well-Paid Freelancer” January 21.2015. -P 29 .

8. https://www.freelancer.com/